Tivoli Public Key Infrastructure

Einführung

Version 3 Release 7.1

Tivoli Public Key Infrastructure

Einführung

Version 3 Release 7.1

Tivoli Public Key Infrastructure Einführung

Copyright Notice

Copyright © 1999, 2001 IBM Corp., einschließlich dieser Dokumentation und aller Software. Alle Rechte vorbehalten. Kann nur gemäß der Softwarelizenzvereinbarung von Tivoli Systems bzw. IBM oder dem Anhang für Tivoli-Produkte der IBM Nutzungsbedingungen verwendet werden. Diese Veröffentlichung darf ohne vorherige schriftliche Genehmigung der IBM Corp. weder ganz noch in Auszügen auf irgendeine Weise - elektronisch, mechanisch, magnetisch, optisch, chemisch, manuell u. a. - vervielfältigt, übertragen, aufgezeichnet, auf einem Abrufsystem gespeichert oder in eine andere Computersprache übersetzt werden. Die IBM Corp. gestattet Ihnen in begrenztem Umfang, eine Hardcopy oder eine Reproduktion einer maschinenlesbaren Dokumentation für den eigenen Gebrauch zu erstellen, unter der Voraussetzung, dass jede dieser Reproduktionen mit dem Copyrightvermerk der IBM Corp. versehen ist. Weitere das Copyright betreffende Rechte werden nur nach vorheriger schriftlicher Genehmigung durch die IBM Corp. gewährt. Die Veröffentlichung dient nicht zu Produktionszwecken. **Die in diesem Dokument aufgeführten Beispiele sollen lediglich zur Veranschaulichung und zu keinem anderen Zweck dienen.**

Bemerkungen

Die vorliegenden Informationen wurden für Produkte und Services entwickelt, die auf dem deutschen Markt angeboten werden. Möglicherweise bietet IBM die in dieser Dokumentation beschriebenen Produkte, Services oder Funktionen in anderen Ländern nicht an. Informationen über die gegenwärtig im jeweiligen Land verfügbaren Produkte und Services sind beim IBM Ansprechpartner erhältlich. Hinweise auf IBM Lizenzprogramme oder andere IBM Produkte bedeuten nicht, daß nur Programme, Produkte oder Dienstleistungen von IBM verwendet werden können. Anstelle der IBM Produkte, Programme oder Dienstleistungen können auch andere ihnen äquivalente Produkte, Programme oder Dienstleistungen verwendet werden, solange diese keine gewerblichen Schutzrechte der IBM verletzen. Die Verantwortung für den Betrieb der Produkte, Programme und Dienstleistungen in Verbindung mit Fremdprodukten liegt beim Kunden, soweit solche Verbindungen nicht ausdrücklich von IBM bestätigt sind.

Für in diesem Handbuch beschriebene Erzeugnisse und Verfahren kann es IBM Patente oder Patentanmeldungen geben. Mit der Auslieferung dieses Handbuchs ist keine Lizenzierung dieser Patente verbunden. Lizenzanforderungen sind schriftlich an IBM Europe, Director of Licensing, 92066 Paris La Defense Cedex, France, zu richten. Anfragen an obige Adresse müssen auf englisch formuliert werden.

Marken

AIX, DB2, DB2 Universal Database, IBM, RS/6000, SecureWay, Tivoli and WebSphere sind in gewissen Ländern eingetragene Marken der International Business Machines Corp. oder von Tivoli Systems Inc.

Das Programm Tivoli PKI (im folgenden als ″Programm″ bezeichnet) enthält Komponenten von IBM WebSphere Application Server und IBM HTTP Web Server (″IBM Server″). Diese dürfen nur zusammen mit dem Programm installiert und entsprechend der für das Programm geltenden Lizenzvereinbarungen in Kombination mit diesem verwendet werden. Die IBM Server müssen auf derselben Maschine wie das Programm installiert sein. Sie sind nicht berechtigt, sie unabhängig vom Programm zu installieren und zu verwenden.

Das Programm Tivoli PKI (im folgenden als ″Programm″ bezeichnet) enthält Komponenten von DB2 Universal Database. Diese Komponenten dürfen nur zusammen mit dem Programm installiert und entsprechend der für das Programm geltenden Lizenzvereinbarungen in Kombination mit diesem verwendet werden, um Daten zu speichern und zu verwalten, die vom Programm verwendet oder generiert werden. Für andere Datenverwaltungsoperationen ist der Einsatz nicht gestattet. Diese Lizenz gilt z. B. nicht für eingehende Verbindungen zur Datenbank, die von anderen Anwendungen aus für Abfragen und Berichtserstellungsoperationen hergestellt werden. Sie sind lediglich zur Installation und Verwendung dieser Komponenten auf der gleichen Maschine berechtigt, auf der auch das Programm installiert und verwendet wird.

Das Programm enthält Komponenten des IBM WebSphere Application Server und des IBM HTTP Web Server (″IBM Server″). Sie sind nicht berechtigt, die IBM Server zu anderen Zwecken als in Verbindung mit der lizenzgerechten Verwendung des Programms zu benutzen. Die IBM Server müssen auf derselben Maschine wie das Programm installiert sein. Sie sind nicht berechtigt, sie unabhängig vom Programm zu installieren und zu verwenden.

Java und alle auf Java basierenden Marken und Logos sind in gewissen Ländern Marken der Sun Microsystems, Inc.

Microsoft, Windows, Windows NT und das Windows-Logo sind in gewissen Ländern Marken der Microsoft Corporation.

UNIX ist eine eingetragene Marke und wird ausschließlich von der X/Open Company Limited lizenziert.

Pentium ist in gewissen Ländern eine Marke der Intel Corporation.

Dieses Programm enthält Sicherheitssoftware von RSA Data Security, Inc. Copyright © 1994 RSA Data Security, Inc. Alle Rechte vorbehalten.

Dieses Programm enthält STL-Software (STL = Standard Template Library) von Hewlett-Packard Company. Copyright (c) 1994.

- Die Berechtigung zum Verwenden, Kopieren, Ändern, Verteilen und Verkaufen dieser Software sowie der zugehörigen Dokumentation für die gewünschten Zwecke wird hiermit gebührenfrei erteilt. Voraussetzung hierfür ist allerdings, daß der o. a. Copyrightvermerk auf allen Kopien erscheint, und daß sowohl dieser Copyrightvermerk als auch dieser Berechtigungshinweis in der zugehörigen Dokumentation aufgeführt werden. Hewlett-Packard Company macht keine Angaben zur Eignung dieser Software für bestimmte Zwecke. Sie wird ohne Modifikationen und ohne Gewährleistung bereitgestellt.

Dieses Programm enthält STL-Software (STL = Standard Template Library) von Silicon Graphics Computer Systems, Inc. Copyright (c) 1996 - 1999.

- Die Berechtigung zum Verwenden, Kopieren, Ändern, Verteilen und Verkaufen dieser Software sowie der zugehörigen Dokumentation für die gewünschten Zwecke wird hiermit gebührenfrei erteilt. Voraussetzung hierfür ist allerdings, daß der o. a. Copyrightvermerk auf allen Kopien erscheint, und daß sowohl dieser Copyrightvermerk als auch dieser Berechtigungshinweis in der zugehörigen Dokumentation aufgeführt werden. Silicon Graphics macht keine Angaben zur Eignung dieser Software für bestimmte Zwecke. Sie wird ohne Modifikationen und ohne Gewährleistung bereitgestellt.

Andere Namen von Unternehmen, Produkten oder Dienstleistungen können Marken oder Dienstleistungsmarken anderer Unternehmen sein.

Inhaltsverzeichnis

Vorwort xi

Zielgruppe xi

Referenzinformationen xii

Inhalt des Handbuchs xiv

Neuerungen im aktuellen Release xv

In diesem Handbuch verwendete Konventionen xvi

Kontaktaufnahme zur Kundenunterstützung xvi

Webinformationen zu Tivoli PKI xvii

Kapitel 1. Tivoli PKI - Einführung 1

Tivoli PKI - Produktbeschreibung 1

Komponenten 3

Tivoli PKI-Server 4

Registrierungsstelle 4

Zertifikatsaussteller 10

Prüfsubsystem 12

Webserver 13

Datenbanksystem 14

Directory-Server 15

IBM 4758 PCI Cryptographic Coprocessor 15

Funktion zur Schlüsselsicherung und -wiederherstellung 17

Funktion für die Massenzertifikatsausstellung 18

Architektur 18

Public Key Infrastructure (PKI) 18

PKIX CMP-Protokoll 19

LDAP-Protokoll 20

Objektspeicher 20

Trust-Modell 21
Codeunterzeichnung 21
Nachrichtenunterzeichnung 21
Datenverschlüsselung. 22
Schlüsselspeicher (KeyStores) 22
Unterstützte Standards 23
Zertifikate gemäß X.509 Version 3. 24

Kapitel 2. Systemvoraussetzungen 27

Softwarevoraussetzungen für den Server 27
Hardwarevoraussetzungen für den Server 29
Voraussetzungen für den Setup Wizard. 31
Client-Voraussetzungen 32

Kapitel 3. Tivoli PKI - Planung 33

Prüfliste für die Installationsplanung 34
System sichern 40
Firewall-Techniken verwenden. 41
Mit Tivoli PKI-Datenbanken arbeiten. 42
IP-Aliasnamen für den Webserver konfigurieren. 44
Mit dem Directory arbeiten 46
Directory-Schema 47
Directory-Zugriffssteuerung 48
Mit dem IBM 4758 PCI Cryptographic Coprocessor arbeiten 49
CA- oder RA-Schlüssel in der Hardware speichern 50
Integration mit dem Policy Director 51
Unterstützte Serverkonfigurationen. 53
Hinweise zu länderübergreifenden Umgebungen. 54
Tivoli PKI-Datenträgerpaket 55

Kapitel 4. Tivoli PKI unter AIX installieren 57

AIX konfigurieren 58
Dateien prüfen. 59
Ausreichende Paging-Bereiche prüfen 60
Fix-Version auf AIX anwenden 61
AIX-Datenträgergruppen und -Dateisysteme konfigurieren 61
CD-ROM-Dateisystem erstellen 63
Anzahl der AIX-Systembenutzer ändern 63
Hostnamensauflösung sicherstellen. 63
Systemimage erstellen 64
Datenbanksoftware installieren. 64
DB2 installieren 65
IBM Directory installieren 67
Directory-Software installieren. 67
Java installieren. 70
WebSphere Application Server-Datenbank erstellen 71
Webserversoftware installieren 72
WebSphere Application Server installieren 72
Upgrade für WebSphere Application Server ausführen 75
Funktion für automatisches Starten des IBM HTTP Server inaktivieren 75
WebSphere Application Server starten 76
IBM 4758 PCI Cryptographic Coprocessor installieren. 77
Tivoli PKI installieren 77
KeyWorks installieren 78
Serversoftware installieren 79
Richtlinien für die Installation auf mehreren Maschinen 82
Bootwerte ändern 86
Konfigurationsprogramm für den Installationsabschluss ausführen 90

Prüfliste für den Installationsabschluss 91
Backup-Dienstprogramm ausführen 92

Kapitel 5. Tivoli PKI unter Windows NT installieren 95

Windows NT konfigurieren 96
Datenbanksoftware installieren 99
Webserversoftware installieren 101
JDK installieren 101
IBM HTTP Server installieren 102
WebSphere Application Server installieren 104
IP-Aliasnamen definieren 105
IBM Directory installieren 105
Directory-Software installieren 105
Directory unter Tivoli PKI verwenden 107
Systemeinstellungen bestätigen 107
Tivoli PKI installieren 108
Serversoftware installieren 109
Bootwerte ändern 111
Konfigurationsprogramm für den Installationsabschluss ausführen 115
Prüfliste für den Installationsabschluss 116
Backup-Dienstprogramm ausführen 117

Kapitel 6. Tivoli PKI konfigurieren 119

Kapitel 7. Erste Schritte 121

Systemverwaltung 122
RA-Verwaltung 123
Registrierung und Zertifizierung 125
Anpassung 126

Glossar **127**

Index **157**

Vorwort

Das vorliegende Handbuch enthält die Informationen, die Sie benötigen, um mit einem Tivoli Public Key Infrastructure-System (Tivoli PKI) produktiv zu arbeiten. Es umfasst die folgenden Themen:

- Einsatz von Tivoli PKI in Ihrem Unternehmen für die verschlüsselte, authentifizierte und vertrauliche Ausführung von Transaktionen über das Internet. Mit Hilfe der Registrierungsfunktion von Tivoli PKI können Sie auf einfache Weise digitale Zertifikate an gesicherte Personen und Einheiten ausstellen und steuern, ob ein Zertifikat erneuert oder widerrufen werden soll.
- Richtlinien für die Tivoli PKI-Planung, beispielsweise für die Integration von Tivoli PKI-Komponenten mit anderen, an Ihrem Standort installierten Produkten.
- Prozeduren zum Installieren des Produkts auf einer IBM AIX-Plattform oder unter Microsoft Windows NT.
- Verweise auf andere Dokumente, die Sie bei der Verwendung der Tivoli PKI-Benutzerschnittstellen und der -Verwaltungs-Tools unterstützen.

Anmerkung: Das aktuelle Release des Produkts wird nur auf AIX-Plattformen unterstützt. Alle Informationen zur Verwendung unter Microsoft Windows können aus diesem Grund ignoriert werden.

Zielgruppe

Das vorliegende Handbuch ist für eine breit gefächerte Zielgruppe konzipiert.

- Marketing-Managern bietet das vorliegende Handbuch Informationen zur Integration von Tivoli PKI in die e-business-Strategie Ihres Unternehmens.
- Sicherheitsmanagern bietet das vorliegende Handbuch Informationen zur Integration von Tivoli PKI in die Netzsicherheitsstrategie Ihres Unternehmens.

- Bei den Informationen für Systemadministratoren wird im vorliegenden Handbuch davon ausgegangen, dass Sie mit der Installation und Konfiguration von Produkten in einer Netzumgebung vertraut sind. Sie sollten über Erfahrung in folgenden Bereichen verfügen:
  - Hardwareinstallation und -konfiguration
  - Internet-Übertragungsprotokolle, vor allem TCP/IP und SSL (Secure Sockets Layer)
  - Verwaltung von Web-Servern
  - PKI-Technologie (PKI = Public Key Infrastructure) einschließlich Directory-Schemata, X.509 Version 3-Standard und Lightweight Directory Access Protocol (LDAP)
  - Relationale Datenbanksysteme und hier insbesondere IBM DB2 Universal Database

Referenzinformationen

Die Tivoli PKI-Produktdokumentation ist im PDF- und HTML-Format auf der Tivoli-Website verfügbar. HTML-Versionen für einige Veröffentlichungen werden zusammen mit dem Produkt installiert. Auf diese kann über die Benutzerschnittstellen zugegriffen werden.

Bitte beachten Sie, dass seit der Veröffentlichung dieser Dokumentationen möglicherweise Änderungen am Produkt vorgenommen wurden. Die neuesten Produktinformationen sowie Informationen zum Zugriff auf eine Veröffentlichung in der gewünschten Sprache und im gewünschten Format finden Sie in den Release-Informationen. Die neueste Version der Release-Informationen ist auf der Website von Tivoli Public Key Infrastructure unter folgender Adresse verfügbar:

`http://www.tivoli.com/support`

Zur Tivoli PKI-Bibliothek gehören die folgenden Dokumentationen:

Einführung

Dieses Buch enthält eine Übersicht über das Produkt. Es listet die Produktvoraussetzungen auf, enthält die Installations-

prozeduren und bietet Informationen zum Zugriff auf die Online-Hilfe, die für die einzelnen Produktkomponenten zur Verfügung steht. Dieses Buch wird in gedruckter Form zusammen mit dem Produkt ausgeliefert.

Systemverwaltung
Dieses Buch enthält allgemeine Informationen zur Verwaltung des Tivoli PKI-Systems. Es umfasst Prozeduren für das Starten und Stoppen der Server, für das Ändern von Kennwörtern, das Verwalten der Server-Komponenten, die Durchführung von Prüfoperationen sowie das Überprüfen der Datenintegrität.

Konfiguration
Dieses Buch enthält Informationen zur Verwendung des Setup Wizard für die Konfiguration eines Tivoli PKI-Systems. Sie können auf die HTML-Version dieses Handbuchs zugreifen, während Sie die Online-Hilfe für den Setup Wizard anzeigen.

Registration Authority Desktop
Dieses Buch enthält Informationen zur Verwendung des RA Desktop für die Verwaltung von Zertifikaten während der gesamten Gültigkeitsdauer. Sie können auf die HTML-Version dieses Handbuchs zugreifen, während Sie die Online-Hilfe für den Desktop anzeigen.

Benutzerhandbuch
Dieses Buch enthält Informationen zum Abrufen und Verwalten von Zertifikaten. Es umfasst Prozeduren für die Verwendung der Browser-Registrierungsformulare von Tivoli PKI für das Anfordern, Erneuern und Widerrufen von Zertifikaten. Darüber hinaus wird in diesem Buch beschrieben, wie eine Vorabregistrierung für PKIX-kompatible Zertifikate durchgeführt wird.

Anpassung
buch enthält Informationen zum Anpassen der Tivoli PKI-Registrierungsfunktion, mit der die Registrierungs- und Zertifizierungszielsetzungen Ihres Unternehmens wirkungsvoll unterstützt werden können.

Sie erfahren z. B., wie HTML- und Java Server-Seiten, Benachrichtigungsbriefe, Zertifikatsprofile und Regel-Exits angepasst werden können.

Inhalt des Handbuchs

Dieses Handbuch enthält die folgenden Informationen:

- „Tivoli PKI - Einführung” auf Seite 1 enthält eine kurze Beschreibung der Funktionen und des Leistungsumfangs von Tivoli PKI, seiner Komponenten sowie der verwendeten Architektur und der unterstützten Standards.
- „Systemvoraussetzungen” auf Seite 27 enthält die Hardware- und Softwarevoraussetzungen, die zur erfolgreichen Installation von Tivoli PKI sowie zum Betrieb des Systems erforderlich sind.
- „Tivoli PKI - Planung” auf Seite 33 enthält allgemeine Informationen zu den Funktionen von Tivoli PKI sowie detaillierte Informationen zu den zu konfigurierenden Komponenten.
- „Tivoli PKI unter AIX installieren” auf Seite 57 enthält Informationen zur Vorgehensweise bei der Installation von Tivoli PKI auf einer AIX-Plattform.
- „Tivoli PKI unter Windows NT installieren” auf Seite 95 enthält Informationen zur Vorgehensweise bei der Installation von Tivoli PKI auf einer Windows NT-Maschine.
- „Tivoli PKI konfigurieren” auf Seite 119 enthält einen Überblick über den Konfigurationsprozess und die Dokumentation, die zur Ausführung der Konfigurationsaufgaben verwendet werden kann.
- „Erste Schritte” auf Seite 121 enthält Erläuterungen zu Themen, Verfahren und Tools, die zum Verwalten und Anpassen verschiedener Komponenten und Funktionen von Tivoli PKI verwendet werden können.
- „Glossar” auf Seite 127 enthält Definitionen der in diesem Handbuch verwendeten Termini und Abkürzungen, die möglicherweise neu oder unbekannt und von Bedeutung sind.

Neuerungen im aktuellen Release

Tivoli PKI 3.7.1 umfasst die folgenden neuen Einrichtungen und Funktionen:

- **Massenzertifikatsausstellung (BCI)**. Diese Funktion dient zur Bereitstellung eines sicheren Verfahrens für authentifizierte Benutzer, mit dessen Hilfe diese mehrere digitale Zertifikate über einen einzigen Tivoli PKI-Aufruf anfordern können.
- **Certificate Management Protocol (CMP) Version 2**. Durch diesen Upgrade auf CMP Version 2 wird für Tivoli PKI eine verbesserte Zuverlässigkeit bei CMP-Statustransaktionen sowie ein höheres Sicherheitsniveau erzielt, als dies unter der zuvor in Tivoli PKI implementierten CMP Version 1 möglich war.
- **Rollover von Root-CA-Schlüsseln**. Diese Funktion ermöglicht dem Zertifikatsaussteller (CA) die Umstellung von einem nicht beschädigten CA-Schlüsselpaar auf das nächste CA-Schlüsselpaar. (Diese Operation wird auch als Aktualisierung des CA-Schlüssels bezeichnet.)
- **Kompatibilität zu LDAP Version 3**. Diese Funktion dient zur Gewährleistung der Schemakompatibilität mit LDAP (Lightweight Directory Access Protocol) Version 3. Sie bietet insbesondere die Möglichkeit, mit Hilfe des in RFC 2256 definierten Directory-Schemas Attribute unter LDAP zu publizieren. Die auf PKIX LDAP Version 2 basierenden Schemata werden weiterhin unterstützt.
- **HSM-Speicherung für RA-Schlüssel**. Diese Funktion erlaubt das Speichern von RA-Schlüsseln in einer HSM-Komponente (HSM = Hardware Security Module) und bietet ein erweitertes Sicherheitsspektrum für RA-Unterschriftsschlüssel.

Änderungen in der Dokumentation des aktuellen Releases werden am Rand mit einer Änderungsmarkierung gekennzeichnet.

Anmerkung: Tivoli PKI 3.7.1 wird nur unter AIX unterstützt. Im aktuellen Release wurde keine Windows NT-Unterstützung implementiert.

In diesem Handbuch verwendete Konventionen

Im vorliegenden Handbuch werden verschiedene Schriftbilder zur Darstellung spezieller Termini und Komponenten verwendet. Diese Konventionen haben folgende Bedeutung:

Konvention	Bedeutung
Fettdruck	Befehle, Schlüsselwörter, Optionen und sonstige Informationen, die exakt so verwendet werden müssen wie dargestellt, werden in **Fettdruck** hervorgehoben.
Kursivdruck	Variablen, die von Ihnen angegeben werden müssen, sowie neue Termini werden in *Kursivdruck* dargestellt. Wörter und Textsegmente, die hervorgehoben werden sollen, erscheinen ebenfalls in *Kursivdruck*.
Monospace-Schrift	Codebeispiele, Ausgabedaten und Systemnachrichten werden in `Monospace-Schrift` dargestellt.

Kontaktaufnahme zur Kundenunterstützung

Wenn bei der Verwendung von Tivoli-Produkten Schwierigkeiten auftreten, können Sie unter der Adresse **http://www.support.tivoli.com** die Homepage der Tivoli-Unterstützungsfunktion aufrufen. Nach der Herstellung der Verbindung und der Übergabe des Kundenregistrierungsformulars können Sie auf zahlreiche Kundenunterstützungsservices im Web zugreifen.

Kunden in Deutschland, Österreich oder der Schweiz können eine der folgenden Telefonnummern anrufen:

- Deutschland: **01805-00-1242**
- Österreich: **01-1706-6000**
- Schweiz: **0800-555454**

Unter diesen Nummern erreichen Sie das Telefonservicecenter der Tivoli-Kundenunterstützung.

Wir sind an Ihren Erfahrungen mit Tivoli-Produkten und der zugehörigen Dokumentation sehr interessiert. Ihre Verbesserungsvorschläge nehmen wir gerne entgegen. Wenn Sie Kommentare oder Vorschläge zur vorliegenden Dokumentation haben, senden Sie diese bitte via E-Mail an pubs@tivoli.com.

Webinformationen zu Tivoli PKI

Tivoli- sowie IBM Tivoli-Kunden können Onlineinformationen für alle Tivoli-Sicherheitsprodukte sowie Tivoli PKI im Web abrufen.

Wichtige Informationen zu den aktuellsten Produktaktualisierungen und Serviceinformationen zu Tivoli PKI finden Sie über die folgende Website:
http://www.tivoli.com/support/secure_download_bridge.html

Informationen zum Produkt Tivoli Public Key Infrastructure finden Sie auf folgender Website:
http://www.tivoli.com/products/index/secureway_public_key/

Informationen zu anderen Tivoli-Sicherheitsverwaltungsprodukten finden Sie auf folgender Website:
http://www.tivoli.com/products/solutions/security/

1

Tivoli PKI - Einführung

Das vorliegende Kapitel enthält eine Übersicht über Tivoli Public Key Infrastructure (Tivoli PKI). Es enthält eine kurze Beschreibung der Funktionen und des Leistungsumfangs von Tivoli PKI, seiner Komponenten sowie der verwendeten Architektur und der unterstützten Standards.

Tivoli PKI - Produktbeschreibung

Tivoli Public Key Infrastructure stellt Anwendungen zur Verfügung, mit denen Benutzer authentifiziert werden können und die gesicherte Übertragung von Daten gewährleistet werden kann. Im Folgenden sind einige Funktionen von Tivoli PKI aufgeführt:

- Das Produkt ermöglicht es Unternehmen, digitale Zertifikate ihren Registrierungs- und Zertifizierungsstrategien entsprechend auszustellen, zu publizieren und zu verwalten.
- Die Unterstützung für die Verschlüsselungsstandards Public Key Infrastructure für X.509 Version 3 (PKIX) und Common Data Security Architecture (CDSA) ermöglicht die Interoperabilität zwischen verschiedenen Lieferanten.
- Digitale Unterschriften und sichere Protokolle bieten die Möglichkeit, alle Teilnehmer einer Transaktion zu authentifizieren.
- Browserbasierte Registrierungsfunktionen bieten optimale Flexibilität.
- Verschlüsselte Kommunikation und gesicherte Speicherung von Registrierungsinformationen stellen die Vertraulichkeit sicher.

Ein Tivoli PKI-System kann auf Serverplattformen unter IBM AIX/6000 (AIX) und Microsoft Windows NT ausgeführt werden. Das Produkt umfasst die folgenden Hauptmerkmale:

- Einen zuverlässigen Zertifikatsaussteller (CA), der die gesamte Gültigkeitsdauer einer digitalen Zertifizierung verwaltet. Um die Authentizität eines Zertifikats zu belegen, unterzeichnet der CA jedes ausgestellte Zertifikat digital. Darüber hinaus werden vom CA auch Zertifikatswiderrufslisten (CRLs) unterzeichnet, um zu bestätigen, dass ein Zertifikat nicht länger gültig ist. Um seinen Unterschriftsschlüssel zusätzlich zu schützen, können Sie Verschlüsselungshardware wie z. B. den IBM 4758 PCI Cryptographic Coprocessor verwenden.
- Eine Registrierungsstelle (RA) führt die administrativen Aufgaben zur Benutzerregistrierung aus. Sie stellt sicher, dass nur solche Zertifikate ausgestellt werden, die Ihre Geschäftsaktivitäten unterstützen, und dass diese Zertifikate ausschließlich an berechtigte Benutzer ausgegeben werden. Diese Verwaltungsaufgaben können mit Hilfe eines automatisierten Prozesses oder durch Mitarbeiter anhand eines entsprechenden Entscheidungsprozesses ausgeführt werden. Ähnlich wie der CA kann die RA auch Verschlüsselungshardwareeinheiten wie z. B. den IBM 4758 PCI Cryptographic Coprocessor verwenden, um ihren Unterschriftsschlüssel zusätzlich zu schützen.
- Eine webbasierte Registrierungsschnittstelle erleichtert das Abrufen von Zertifikaten für Browser, Server, VPNs (Virtual Private Networks), Smart-Cards und die gesicherte Übertragung von E-Mails.
- Die webbasierte Verwaltungsschnittstelle RA Desktop ermöglicht berechtigten Registratoren das Genehmigen oder Zurückweisen von Registrierungsanforderungen sowie das Verwalten von bereits ausgestellten Zertifikaten.

- Ein Prüfsubsystem berechnet einen Nachrichtenauthentifizierungscode (Message Authentication Code, MAC) für jeden Protokolleintrag. Wenn Prüfdaten geändert oder gelöscht werden, nachdem sie in der Prüfdatenbank aufgezeichnet wurden, kann mit Hilfe des MAC der unberechtigte Zugriff festgestellt werden.
- Regel-Exits und BPOs (Unternehmensprozessobjekte) ermöglichen Anwendungsentwicklern die Anpassung des Registrierungsprozesses.
- Integrierte Unterstützung für eine kryptografische Maschine. Um die Kommunikation zu authentifizieren, sind die Hauptkomponenten von Tivoli PKI werksseitig mit einem privaten Schlüssel unterzeichnet. Sicherheitsobjekte, wie beispielsweise Schlüssel und MACs, sind verschlüsselt und in geschützten Bereichen gespeichert, die als Schlüsselspeicher (KeyStores) bezeichnet werden.
- Integrierte Unterstützung für das IBM Directory. Im Directory sind Informationen zu gültigen und widerrufenen Zertifikaten in einem mit LDAP kompatiblen Format gespeichert.
- Integrierte Unterstützung für IBM WebSphere Application Server und IBM HTTP Server. Der Web-Server kooperiert mit dem RA-Server bei der Verschlüsselung von Nachrichten, der Authentifizierung von Anforderungen und der Übertragung von Zertifikaten an den gewünschten Empfänger.
- Integrierte Unterstützung für IBM DB2 Universal Database.

Komponenten

Im folgenden Diagramm wird ein Tivoli PKI-System dargestellt, bei dem die Serverprogramme auf drei unterschiedlichen Maschinen verteilt sind. In Ihrem Unternehmen können die drei Server auch auf einer einzigen Maschine installiert sein.

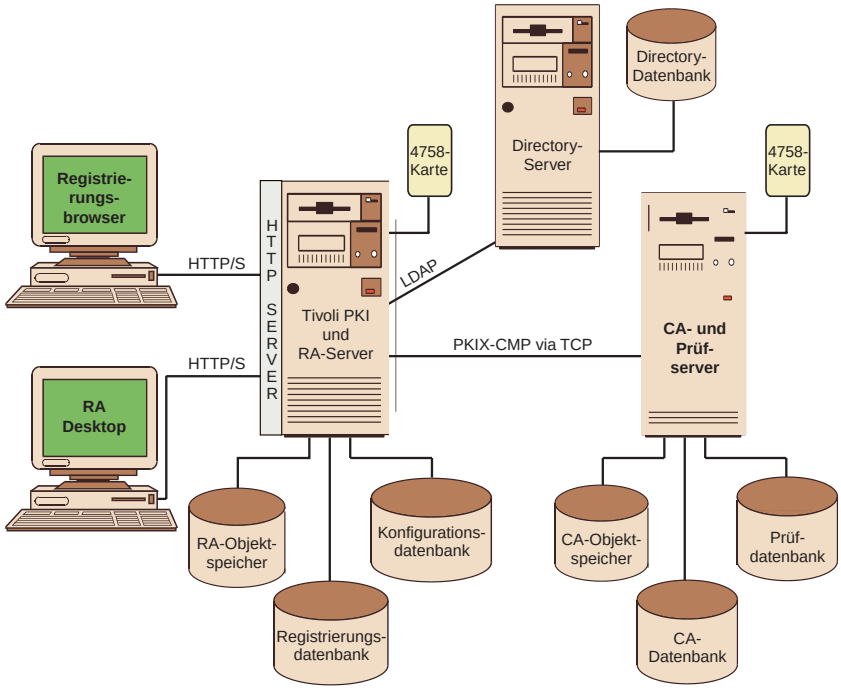

Abbildung 1. Komponentenkonfiguration bei Tivoli PKI

Tivoli PKI-Server

Der Tivoli PKI-Server ist der zentrale Server, über den die anderen Komponenten miteinander verbunden sind. Dieser Server verwaltet die Konfigurationsdatenbank und stellt die Dienstprogramme für die Systemverwaltung zur Verfügung.

Registrierungsstelle

Die Registrierungsstelle (RA) ist die Server-Komponente, die den Registrierungsprozess verwaltet. Die RA gewährleistet, dass Zertifikate nur an genehmigte Entitäten ausgestellt werden. Darüber hinaus wird von dieser Instanz sichergestellt, dass die ausgestellten Zertifikate nur für autorisierte Zwecke verwendet werden. Die RA dient zur Ausführung der folgenden wichtigen Aufgaben:

- Bestätigen der Identität der anfordernden Entität

- Überprüfen, ob der Antragsteller über die Berechtigung für ein Zertifikat verfügt, das die angeforderten Attribute und Berechtigungen enthält
- Genehmigen und Zurückweisen von Anforderungen zur Erstellung, Erneuerung oder zum Widerrufen von Zertifikaten
- Überprüfen, ob eine Entität, die auf eine gesicherte Anwendung oder Ressource zugreifen möchte, über den privaten Schlüssel verfügt, der dem öffentlichen Schlüssel für das verwendete Zertifikat zugeordnet ist

Ähnlich wie der Tivoli PKI-CA kann die RA auch Verschlüsselungshardwareeinheiten wie z. B. den IBM 4758 PCI Cryptographic Coprocessor verwenden, um ihre Unterschriftsschlüssel zusätzlich zu schützen.

Bei Tivoli PKI stellt die auf dem RA-Server installierte Registrierungsfunktion die Basis zur Verfügung, auf der eine breite Palette von Registrierungsaktivitäten unterstützt wird. Während der Konfiguration des Systems wird eine Registrierungsdomäne eingerichtet, die die Geschäfts- und Zertifikatsregeln sowie die Ressourcen in Übereinstimmung mit den bevorzugten Registrierungs- und Zertifizierungsstrategien Ihres Unternehmens steuert.

Registrierung

Die RA bietet Unterstützung für eine Vielzahl verschiedener Registrierungsprotokolle und Zertifikatstypen. Die Registrierungsfunktionen umfassen folgendes:

- Verwendung einer DB2-Datenbank für die Protokollierung verschlüsselter Registrierungs- und Zertifikatsdaten.
- Unterstützung für manuelle und automatische Prozesse zur Registrierungsgenehmigung.
- Eine Gruppe von Registrierungsformularen auf Java-Basis, mit denen Benutzer Zertifikate über die eigenen Web-Browser anfordern und abrufen können. Durch den Registrierungsprozess wird die Identität des Clients und des Servers authentifiziert, und die Zertifikate werden an genehmigte Entitäten übergeben, wobei alle angeforderten Daten während der gesamten Kommunikation

zwischen Absender und Empfänger verschlüsselt werden. Der Registrierungsprozess umfasst Folgendes:

- Die Übergabe von Zertifikaten über SSL (Secure Sockets Layer) zur Verwendung bei Anwendungen, auf die über einen Web-Browser oder einen Web-Server zugegriffen wird.
- Die Übergabe von Zertifikaten über PKIX CMP (Certificate Management Protocol) zur Verwendung in PKIX-Client-Anwendungen oder zum Speichern auf Smart-Cards.
- Die Übergabe von Zertifikaten, die den IPSec-Standard (IPSec = Internet Protocol Security) unterstützen, zur Verwendung bei sicheren VPN-Anwendungen oder IPSec-fähigen Einheiten.
- Die Übergabe von Zertifikaten, die S/MIME (Secure Multipurpose Internet Mail Extensions) unterstützen, zur Verwendung bei sicheren E-Mail-Anwendungen.
- Die Übergabe von Benachrichtigungsschreiben, in denen der Antragsteller über die Genehmigung bzw. die Ablehnung einer Anforderung informiert wird.

- Eine Gruppe von Zertifikatsprofilen, die das Abrufen des gewünschten Zertifikatstyps für den Benutzer vereinfachen. In den Profilen sind der geplante Verwendungszweck und der Gültigkeitszeitraum des Zertifikats definiert. Auf der Basis der Informationen in der Schablone kann die RA ein Zertifikat im korrekten Format mit dem erforderlichen Zertifikatsinhalt zur Verfügung stellen.

  Informationen zu den Zertifikatstypen und Zertifikatserweiterungen, die von der RA unterstützt werden, finden Sie in den Abschnitten „Unterstützte Standards” auf Seite 23 und „Zertifikate gemäß X.509 Version 3” auf Seite 24.

- Unterstützung für die Vorabregistrierung, einen Prozess, der es einem Benutzer - normalerweise einem Administrator - ermöglicht, ein PKIX-kompatibles Zertifikat für einen anderen Benutzer anzufordern.
- Unterstützung für Regel-Exits und BPOs (Unternehmensprozessobjekte). Mit diesen Komponenten können Unternehmen wäh-

rend des Registrierungsprozesses eigene Programme aufrufen. Die RA enthält einen Beispielregel-Exit, der die automatische Genehmigungsverarbeitung ausführt.

Informationen zum Entwickeln und Anpassen von Unternehmensprozessobjekten (BPOs) an Ihre individuellen Unternehmensanforderungen finden Sie im IBM Redbook *Working with Business Process Objects for Tivoli SecureWay PKI*, IBM Form SG24-6043-00.

Vollständige Informationen zur Verwendung eines Webbrowsers für die Zertifikatsregistrierung finden Sie im *Tivoli PKI Benutzerhandbuch*. Dieses Buch enthält darüber hinaus eine Beschreibung der Zertifikatstypen, die mit der Standardinstallation von Tivoli PKI zur Verfügung stehen.

Verwaltung

Mit dem Applet RA Desktop können berechtigte Administratoren (Registratoren) Zertifikatsanträge überprüfen, Anforderungen genehmigen oder zurückweisen, Zertifikate erneuern und permanent oder temporär widerrufen. Das Applet unterstützt die folgenden Aufgaben:

- Anstehende Registrierungsanforderungen abrufen.
- Die Registrierungsdatenbank abfragen, um Datenbanksätze abzurufen, die bestimmten Kriterien entsprechen, und um die entsprechenden Aktionen für diese Sätze auszuführen.
- Detaillierte Informationen zu einem Zertifikat oder einer Zertifikatsanforderung überprüfen, wie beispielsweise das Protokoll für alle Aktionen, die seit der ersten Übergabe einer Anforderung ausgeführt wurden.
- Den Gültigkeitszeitraum für ein Zertifikat definieren.
- Einen Datenbanksatz mit Anmerkungen versehen, um eine Aktion zu begründen.

Der RA Desktop ist ein sicheres Applet. Ein Benutzer kann lediglich als berechtigter Registrator darauf zugreifen. Tivoli PKI stellt ein Tool zur Verfügung, durch das dieser Prozess vereinfacht wird. Es

kann eine beliebige Anzahl von Registratoren hinzugefügt werden, um das Arbeitsaufkommen an Registrierungen zu bearbeiten.

Wenn Sie einen Registrator hinzufügen, müssen Sie die entsprechende Registrierungsdomäne definieren und die Berechtigungen für diesen Benutzer angeben. So können Sie beispielsweise einen Registrator ausschließlich für das Genehmigen und Ablehnen von Anforderungen berechtigen, während Sie einem anderen Registrator darüber hinaus die Berechtigung für das Widerrufen von Zertifikaten erteilen.

- Informationen dazu, wie Sie das Applet RA Desktop installieren und verwenden sowie auf dieses zugreifen können, finden Sie im Handbuch *Tivoli PKI RA Desktop*.
- Informationen zum Berechtigen von Registratoren finden Sie im Handbuch *Tivoli PKI Systemverwaltung*.

Anpassung

Sie können die zum Lieferumfang von Tivoli PKI gehörende Registrierungsfunktion verwenden, ohne sie anzupassen. Möglicherweise sollen jedoch einige der Registrierungsformulare oder -prozesse angepasst werden, um der speziellen Zielsetzung des jeweiligen Unternehmens für die digitale Zertifizierung zu entsprechen. So kann beispielsweise das Firmenlogo auf dem Browser-Registrierungsformular angezeigt werden. Darüber hinaus ist es möglich, die Zertifikatsprofile so zu ändern, dass sie die Zertifikatserweiterungen unterstützen, die für die zu registrierenden Benutzer-, Server- oder Einheitenklassen relevant sind.

Nach der Installation und Konfiguration von Tivoli PKI können Sie eine größere Anzahl der Dateien kopieren, durch die Ihre Registierungsdomäne definiert wird, und sie für Ihre Unternehmensstrategie anpassen. Erstellen Sie vor der Änderung einer Datei unbedingt eine Sicherungskopie.

Sie können die nachfolgend aufgeführten Dateien der Registrierungsfunktion kopieren oder aktualisieren. Während der Konfiguration werden diese Dateien in dem Verzeichnispfad erstellt, der für Ihre Registrierungsdomäne definiert wurde.

- Die Konfigurationsdateien (Dateityp .cfg), die im Unterverzeichnis etc installiert sind. In diesen Dateien können beispielsweise die Laufzeiteinstellungen für den RA-Server oder RA Desktop angepasst werden.
- Die Beispiele für Benachrichtigungsschreiben (Dateityp .ltr), die im Unterverzeichnis etc installiert sind. Tivoli PKI stellt Beispieltext für Benachrichtigungsschreiben zur Verfügung, in denen Benutzer darüber informiert werden, wenn eine Anforderung genehmigt oder widerrufen wurde. Sie können jedoch auch ein eigenes Schreiben verfassen.
- Die HTML- (Dateityp .html), Grafik- (Dateityp .gif) und Java Server Pages-Dateien (Dateityp .jsp), die im Unterverzeichnis 'webpages' installiert sind. Sie können beispielsweise den Text und die Grafiken ändern, die in den Browser-Registrierungsformularen angezeigt werden. Außerdem können Sie ein vorhandenes Zertifikatsprofil anpassen oder ein neues Profil definieren, das den Zertifikatsregeln Ihres Unternehmens entspricht.
- Der Regel-Exit (policy_exit), der im Unterverzeichnis bin installiert ist. Tivoli PKI stellt diesen Exit als Beispiel dafür zur Verfügung, wie die automatische Genehmigungsverarbeitung zu implementieren ist. Sie können andere Exits schreiben, durch die die Registrierungsverarbeitung in andere Anwendungen integriert wird, oder durch die eigene Registrierungsaktionen verarbeitet werden.

Informationen zu den Änderungen, die Sie an den Registrierungs- und Zertifizierungsprozessen vornehmen können, sowie Anweisungen zur Vorgehensweise finden Sie im Handbuch *Tivoli PKI Anpassung*.

Zusätzliche Informationen zur Anpassung finden Sie im IBM Redbook *Working with Business Process Objects for Tivoli SecureWay PKI*, IBM Form SG24-6043-00. Diese Veröffentlichung enthält Empfehlungen zum Entwickeln und Anpassen von BPOs (Unternehmensprozessobjekten) an die individuellen Anforderungen Ihres Unternehmens.

Zertifikatsaussteller

Der Zertifikatsaussteller (CA) ist die Server-Komponente, die den Zertifizierungsprozess verwaltet. Er stellt dabei eine anerkannte dritte Partei für die Benutzer dar, die e-business-Aktionen ausführen und bürgt über die von ihm ausgestellten Zertifikate für die Identität von Benutzern. Das Zertifikat weist nicht nur die Identität des Benutzers nach, es enthält außerdem einen öffentlichen Schlüssel, mit dem der Benutzer die Kommunikation prüfen und verschlüsseln kann.

Die Vertrauenswürdigkeit der einzelnen Parteien hängt von der Anerkennung des CAs ab, der die verwendeten Zertifikate ausgestellt hat. Um die Integrität eines Zertifikats sicherzustellen, wird dieses vom CA digital unterzeichnet. Durch Versuche, ein Zertifikat zu ändern, wird die Unterschrift ungültig und das Zertifikat unbrauchbar.

Der Tivoli PKI-CA stellt mit Hilfe der folgenden Methoden eine sichere Transaktionsumgebung zur Verfügung:

- Sicherstellen der Eindeutigkeit eines Zertifikats. Der CA generiert eine Seriennummer für alle neuen sowie alle erneuerten Zertifikate. Diese Seriennummer ist eine eindeutige Kennung, die nicht als Teil des registrierten Namens (Distinguished Name, DN) im Zertifikat gespeichert wird.
- Protokollieren der ausgestellten Zertifikate. Der CA verwaltet eine Liste der ausgestellten Zertifikate (ICL). Mit der ICL wird eine (über Seriennummern indexierte) sichere Kopie jedes Zertifikats in einer DB2-Datenbank gespeichert.
- Protokollieren widerrufener Zertifikate. Der CA erstellt und aktualisiert Zertifikatswiderrufslisten (CRLs). Der CA und die RA tauschen Nachrichten aus, sobald ein Zertifikat widerrufen wird; so kann die RA das Directory bei der nächsten regelmäßigen Aktualisierung entsprechend aktualisieren. Alle Zertifikatswiderrufslisten werden vom CA digital unterzeichnet, um deren Integrität zu überprüfen.
- Gewährleisten eines Schutzes gegen die Manipulation von Daten. Der CA generiert für alle in die Datenbank geschriebenen Sätze einen Nachrichtenauthentifizierungscode (MAC). Mit Hilfe des MAC kann festgestellt werden, wenn Daten in der Datenbank

geändert oder gelöscht wurden. Auf diese Weise wird die Datenbankintegrität sichergestellt.

- Schützen der CA-Unterschrift. Der CA kann mit dem IBM 4758 PCI Cryptographic Coprocessor integriert werden. Der IBM 4758 PCI Cryptographic Coprocessor verwendet einen fest gespeicherten Chiffrierschlüssel, um den Unterschriftsschlüssel des CA zu verschlüsseln und damit zu schützen.
- Unterstützen der Aktualisierung (Rollover) des CA-Schlüsselpaares und des zugehörigen Zertifikats zur Verhinderung des Ablaufens.
- Unterstützen der Funktionen zur Überprüfung und Datenwiederherstellung. Der CA generiert für zahlreiche überprüfbare Ereignisse Prüfsätze. Der Prüfserver speichert diese Sätze in einer DB2-Datenbank.
- Wenn in Ihrem Unternehmen diskrete Anwendungen verwendet werden, für die ein einzelner CA ausreicht, unterstützt Tivoli PKI selbstunterzeichnete CA-Zertifikate. In diesem Szenario ist der CA für die gesamte Zertifizierung innerhalb seiner Verwaltungsdomäne verantwortlich.
- Wenn in Ihrem Unternehmen verzahnte oder hierarchische Berechtigungsketten vorliegen, können sie den CA so konfigurieren, dass er mit anderen CAs zusammenarbeitet.
  - Ein Tivoli PKI-CA kann zusammen mit einem anderen CA eine gegenseitige Zertifizierung durchführen und vereinbaren, dass die vom jeweiligen Partner-CA unterzeichneten Zertifikate als Authentizitätsbeleg akzeptiert werden. Die gegenseitige Zertifizierung ermöglicht Entitäten in der Verwaltungsdomäne eines CAs die sichere Kommunikation mit den Entitäten in der Verwaltungsdomäne eines anderen CAs.
  - Ein Tivoli PKI-CA kann als Root-CA andere CA-Zertifikate unterzeichnen. Darüber hinaus unterstützt er Anforderungen von anderen CAs, die dessen CA-Zertifikat unterzeichnen möchten. Dadurch kann der CA in eine Sicherheitshierarchie integriert werden. Er akzeptiert Zertifikate, die von einem

beliebigen, in der Hierarchie über ihm stehenden CA unterzeichnet wurden, als Authentizitätsnachweis.

Solche Sicherheitsmodelle empfehlen sich beispielsweise bei der Unterteilung von geographischen Bereichen oder Organisationseinheiten in bestimmte Verwaltungsdomänen. Auf diese Weise können außerdem verschiedene Zertifikatsregeln für unterschiedliche Unternehmensbereiche angewandt werden.

- Wenn Sie in Ihrem Unternehmen Zertifikate für Zwecke benötigen, die nicht bereits durch die Tivoli PKI-Zertifikatsprofile unterstützt werden, kann der CA Zertifikate mit kundendefinierten Erweiterungen generieren und auf ihre Gültigkeit hin überprüfen.

  Das Handbuch *Tivoli PKI Anpassung* enthält Informationen zur Definition neuer Zertifikatsprofile sowie zur Definition von Zertifikatserweiterungen.

Ausführlichere Informationen zum Tivoli PKI-CA finden Sie im Handbuch *Tivoli PKI Systemverwaltung*. Dieses Buch enthält Richtlinien zum Anpassen der Laufzeitoptionen für den CA-Server sowie Prozeduren zum Herstellen von gegenseitig zertifizierten und hierarchisch strukturierten CA-Trust-Modellen.

Prüfsubsystem

In Tivoli PKI stellt das Prüfsubsystem Unterstützung für die Protokollierung sicherheitsrelevanter Aktionen zur Verfügung. Der Prüf-Server führt die folgenden Aktionen im Rahmen der Prüfungsaktivität aus:

- Empfangen von Prüfereignissen von Prüf-Clients wie z. B. von der Registrierungsstelle und dem Zertifikatsaussteller.
- Aufzeichnen von Ereignissen in einem Prüfprotokoll, das normalerweise in einer DB2-Datenbank gespeichert wird. (Das Protokoll kann wahlweise auch als Datendatei gespeichert werden.) Das Protokoll enthält für jedes Prüfereignis einen Protokolleintrag.
- Ermöglichen der Verwendung einer Maske, mit der Prüf-Clients bestimmte Prüfereignisse abschirmen können. Zwar werden

einige Ereignisse stets protokolliert, für andere kann jedoch mit Hilfe einer Maske die Aufzeichnung verhindert werden. Dadurch können Sie die Größe der Prüfprotokolle steuern und sicherstellen, dass nur die Ereignisse protokolliert werden, die relevant sind.

- Berechnen eines Nachrichtenauthentifizierungscodes (MAC) für alle Prüfsätze. Mit Hilfe des MAC kann die Integrität des Datenbankinhalts gewährleistet werden. So können Sie beispielsweise anhand des MAC feststellen, ob ein Eintrag seit seiner Protokollierung geändert, unbefugt manipuliert oder gelöscht wurde.
- Bereitstellen eines Tools zur Durchführung von Integritätsprüfungen der Prüfdatenbank und der archivierten Prüfsätze.
- Bereitstellen eines Tools zum Archivieren und Unterzeichnen des aktuellen Status der Prüfdatenbank. Aus Sicherheitsgründen sollten Sie die Prüfdatenbank regelmäßig archivieren und separat speichern. Durch die Archivierung der Datenbank kann auch eine Leistungsverbesserung erzielt und Plattenspeicherplatz gespart werden.

Der Prüf-Server muss auf derselben Maschine installiert sein wie der Zertifikatsaussteller. Nach der Installation und Konfiguration des Systems finden Sie im Handbuch *Tivoli PKI Systemverwaltung* Informationen zur Verwendung der Prüf-Tools sowie zur Verwaltung des Prüf-Servers.

Webserver

Tivoli PKI verwendet den IBM WebSphere Application Server, um eine gesicherte Basis für Netztransaktionen bereitzustellen. Bei WebSphere handelt es sich um eine Gruppe von Produkten, bei denen die Gewährleistung der System- und Datensicherheit von zentraler Bedeutung ist. Diese Produktgruppe umfasst den IBM HTTP Server, der die Implementierung von hoch entwickelten e-business-Anwendungen unterstützt.

In einem Tivoli PKI-System muss die Web-Server-Software auf derselben Maschine installiert werden wie die Registrierungsstelle. Auf dieses Weise wird eine sichere Grenze zwischen den geschützten

Programmen und den Benutzern eingerichtet, die auf diese Programme zugreifen möchten. Mit Hilfe der HTTP-, HTTPS- und SSL-Technologie kann der Web-Server die Kommunikation zwischen den Clients und dem Server verschlüsseln. Er kann darüber hinaus die Verbindungen authentifizieren, um unberechtigten Zugriff oder unbefugtes Ändern von Daten zu verhindern.

Der Web-Server verwendet verschiedene Anschlüsse, um unterschiedliche Anforderungstypen zu verarbeiten:

- Einen öffentlichen Anschluss für Anforderungen, für die keine Verschlüsselung oder Authentifizierung erforderlich ist.
- Einen gesicherten Anschluss für Anforderungen, für die eine Verschlüsselung und eine Server-Authentifizierung erforderlich sind.
- Einen gesicherten Anschluss für Anforderungen, für die eine Verschlüsselung, eine Server-Authentifizierung und eine Client-Authentifizierung erforderlich ist.

In einem Tivoli PKI-System verarbeitet der Web-Server alle Anforderungen, die er von einem Web-Browser erhält. Hierzu gehören Anforderungen für neue Zertifikate, Anforderungen für die Erneuerung oder den Widerruf vorhandener Zertifikate sowie Anforderungen für die Ausführung sicherer Applets. Falls erforderlich, führt der Web-Server eine Authentifizierung durch, bevor er den Informationsaustausch zulässt.

Datenbanksystem

IBM DB2 Universal Database (DB2) dient bei Tivoli PKI als das grundlegende System zur Datenspeicherung. Die Server-Komponenten verwalten separate Datenbanken für Konfigurationsdaten, Registrierungsdaten, Zertifikatsdaten, Prüfdaten und Directory-Daten. DB2 bietet umfassende Sicherheitseinrichtungen und verfügt über eine hohe Speicherkapazität. So ermöglicht DB2 beispielsweise Tivoli PKI, Registrierungsdaten im verschlüsselten Format zu speichern und Integritätsprüfungen für gespeicherte Prüfsätze durchzuführen.

Die DB2-Version, die unter Tivoli PKI benötigt wird, ist in dem Tivoli PKI-Datenträgerpaket enthalten. Vor der Installation des Tivoli

PKI-Server-Codes muss sichergestellt werden, dass die Datenbanksoftware auf allen Maschinen zur Verfügung steht, auf denen eine Server-Komponente installiert werden soll. Während der Installation und Konfiguration werden die erforderlichen Datenbanken von Tivoli PKI erstellt.

Directory-Server

Das IBM Directory verwaltet Zertifikatsinformationen an zentraler Stelle. Durch die Integration mit IBM DB2 kann das Directory Millionen von Verzeichniseinträgen unterstützen. Darüber hinaus ermöglicht es Client-Anwendungen, wie beispielsweise Tivoli PKI, Transaktionen zum Speichern in der Datenbank, zum Aktualisieren der Datenbank und zum Abrufen von Informationen aus der Datenbank durchzuführen.

In Tivoli PKI publiziert der RA-Server die folgenden Informationen im Directory:

- Zertifikate für öffentliche Schlüssel, die zur Verschlüsselung und Authentifizierung verwendet werden
- Die einem registrierten Namen (DN) zugeordneten Attribute (die Aufgabenbereiche und Berechtigungen des Eigners)
- Zertifikatswiderrufslisten, die die Seriennummern aller widerrufenen Zertifikate enthalten
- Informationen zu dem CA, der die Zertifikate unterzeichnet, einschließlich der Unternehmens- und Zertifikatsregeln, die dem Zertifikat zugeordnet sind

IBM 4758 PCI Cryptographic Coprocessor

Wenn ein CA ein Zertifikat ausstellt, wird durch die Unterschrift des CA bestätigt, dass der Benutzer berechtigt ist, auf die Services zuzugreifen, für die er registriert ist. Der Unterschriftsschlüssel des CA muss geschützt werden, um zu verhindern, dass unbefugte Benutzer Zertifikate erhalten und auf sensible Ressourcen zugreifen können. Ähnliche Sicherheitsfaktoren gelten auch für die von der RA generierten Schlüsselpaare.

Durch die Anwendung von Verschlüsselungsverfahren können Softwarelösungen einen hohen Grad an Sicherheit für Unterschriftsschlüssel bieten. Da die Schlüssel jedoch unverschlüsselt vorliegen müssen, um die zugehörige Unterschrift zu generieren, sind diese damit dem Zugriff durch nicht berechtigte Benutzer ausgesetzt.

Beim IBM 4758 PCI Cryptographic Coprocessor handelt es sich um eine spezielle Hardwareeinheit, die in einem Tivoli PKI-System dazu verwendet werden kann, CA- und RA-Schlüssel zu schützen. Er implementiert umfassende RSA- und DES-gestützte Verschlüsselungsfunktionen innerhalb eines geschlossenen, manipulationssicheren Hochsicherheitsprozessors, der in die Hardware integriert ist. Der Koprozessor gewährleistet den Datenschutz durch die Anwendung von Verschlüsselungsverfahren und bietet darüber hinaus Funktionen für die Schlüsselverwaltung und Unterstützung für angepasste Anwendungen. Er unterstützt außerdem die MD5- und SHA-1-Hash-Algorithmen. Diese Funktionen gewährleisten, dass der IBM 4758 PCI Cryptographic Coprocessor den brancheninternen Anforderungen für Standards und Anwendungen entspricht, die über HSM-Funktionen (HSM = Hardware Security Module) verfügen müssen.

Bei einer Tivoli PKI-Installation, bei der alle Komponenten auf einer einzigen Maschine implementiert sind, können für CA und RA jeweils eigene 4758-Koprozessorkarten benutzt oder es kann eine Karte gemeinsam verwendet werden. Sie können bei der Ausführung des Setup Wizard angeben, wie die Karte konfiguriert werden soll.

Anmerkung: Die Unterstützung für den IBM 4758 PCI Cryptographic Coprocessor steht nur in der AIX-Version von Tivoli PKI zur Verfügung.

Das Handbuch *Tivoli PKI Systemverwaltung* und die Produktdokumentation enthalten zusätzliche Informationen zum IBM 4758 PCI Cryptographic Coprocessor.

Empfehlung

Der IBM 4758 PCI Cryptographic Coprocessor ist zwar keine erforderliche Komponente, es wird jedoch von IBM empfohlen, ihn auf demselben Server zu installieren, auf dem auch der Zertifikatsaussteller installiert werden soll. Wenn Sie für den Schutz der CA-Schlüssel die Softwareverschlüsselung verwenden, können Sie die Hardwareunterstützung nicht zu einem späteren Zeitpunkt installieren, ohne die Tivoli PKI-Software ebenfalls erneut zu installieren.

Funktion zur Schlüsselsicherung und -wiederherstellung

Tivoli PKI stellt eine Funktion bereit, mit der Anforderungen zum Sichern und Wiederherstellen von Schlüsseln verarbeitet werden können. Mit dieser Funktion können Endentitätszertifikate sowie entsprechende, von Tivoli PKI zertifizierte private Schlüssel gesichert und wiederhergestellt werden.

Diese Funktion ermöglicht die Wiederherstellung verlorener, vergessener oder aus anderen Gründen nicht mehr verfügbarer Zertifikate und privater Schlüssel. Beispiel: Ein Mitarbeiter ist für die routinemäßige Erstellung von Sicherungskopien für Zertifikate und private Schlüssel verantwortlich und scheidet unvorhergesehener Weise aus dem Unternehmen aus. Hierbei versäumt er, alle privaten Schlüssel zurückzugeben, die für den Zugriff auf die Zertifikate erforderlich sind. Durch die Ausgabe einer Wiederherstellungsanforderung können diese Informationen wieder bereitgestellt werden.

Für den Sicherungsprozess muss der Benutzer eine PKCS #12-Datei erstellen. Diese Datei enthält das Zertifikat sowie den privaten Schlüssel des Benutzers. Der Benutzer gibt über einen unterstützten Browser eine Sicherungsanforderung aus und verwendet hierbei die PKCS #12-Datei als Eingabe. Die Datenbank für die Schlüsselwiederherstellung (krbdb) wird daraufhin aktualisiert und enthält nun die Zugriffsinformationen. Bei der Wiederherstellung von Schlüsseln wird ähnlich vorgegangen. Sie geben eine Wiederherstellungsan-

forderung aus und definieren hierbei das Kennwort für die PKCS #12-Datei, die gesichert wurde. Nach der Genehmigung der Anforderung durch den RA-Administrator können Sie diese Datei herunterladen.

Funktion für die Massenzertifikatsausstellung

Tivoli PKI bietet eine Funktion für die Massenzertifikatsausstellung, mit der der Kunde eine große Anzahl von Endentitätszertifikaten in einem einzigen, automatisierten Arbeitsgang registrieren, erstellen und an LDAP (Lightweight Directory Access Protocol) übertragen kann. Für diese Funktion ist eine korrekt formatierte Eingabedatei erforderlich, in der Zertifikatsinformationen einschließlich der Angaben zum öffentlichen Schlüssel gespeichert sind. Während des Prozesses wird die Eingabe in die Registrierungsdatenbank eingelesen. Anschließend werden die Anforderungen zur Generierung des benötigten Zertifikats an den CA gesendet und danach werden die Benutzerdaten und das Zertifikat an das Directory gesendet. Die Funktion für die Massenzertifikatsausstellung kann als Einzelprozess ausgeführt oder in separate Prozesse aufgeteilt werden. Welches Verfahren hierbei ausgewählt wird, hängt vom Unternehmensmodell des jeweiligen Kunden ab. Detaillierte Informationen zu dieser Funktion finden Sie im Handbuch *Tivoli PKI Systemverwaltung*.

Architektur

Die folgenden Abschnitte enthalten Informationen zum Architekturgerüst von Tivoli PKI sowie zu den unterstützten Protokollen.

Public Key Infrastructure (PKI)

PKI (Public Key Infrastructure) stellt Anwendungen ein Gerüst für die Durchführung der folgenden Sicherheitsaktivitäten zur Verfügung:

- Authentifizierung aller Teilnehmer an elektronischen Transaktionen
- Erteilen von Zugriffsberechtigungen für sensible Systeme und Repositories
- Überprüfen der Autoren aller Nachrichten mit Hilfe der digitalen Unterschrift
- Verschlüsseln des Inhalts der gesamten Kommunikation

Der PKIX-Standard wurde auf der Basis von PKI entwickelt, um die Interoperabilität von e-business-Anwendungen zu unterstützen. Der Hauptvorteil dieses Standards liegt darin, dass er Unternehmen ermöglicht, gesicherte elektronische Transaktionen unabhängig von der verwendeten Betriebsumgebung oder Anwendungssoftware durchzuführen.

Die PKIX-Implementierung in Tivoli PKI basiert auf der Common Data Security Architecture (CDSA) von Intel. CDSA unterstützt eine Vielzahl von Sicherheitsmodellen, Zertifikatsformaten, Verschlüsselungsalgorithmen und Zertifikats-Repositories. Unternehmen können mit Hilfe dieser Architektur Anwendungen erstellen, die dem PKI-Standard entsprechen und ihre Unternehmensstrategien unterstützen. Diese Fähigkeit stellt den Hauptvorteil von CDSA dar.

PKIX CMP-Protokoll

Tivoli PKI verwendet das PKIX Certificate Management Protocol (CMP) für die Kommunikation zwischen den RA- und CA-Servern sowie für die Kommunikation zwischen dem RA-Server und den Clients. CMP verwendet als primäres Übertragungsprotokoll TCP/IP, es steht jedoch auch eine Abstraktionsebene oberhalb der Sockets-Schicht zur Verfügung. Dies ermöglicht die Unterstützung für zusätzliche Datenübertragungsoperationen mit Sendeaufrufen (Polling).

CMP definiert Nachrichtenformate für die gesamte Gültigkeitsdauer eines Zertifikats. Darüber hinaus definiert CMP, wie der Nachrichtenschutz unabhängig vom Übertragungsprotokoll ausgeführt werden soll.

CMP Version 2, das im aktuellen Release von Tivoli PKI unterstützt wird, trägt zur Verbesserung der Interoperabilität bei und ermöglicht den Einsatz von CAs unterschiedlicher Hersteller bei der Ausführung verschiedenster Funktionen wie z. B. der Ausstellung, Überarbeitung und dem Widerruf von digitalen Zertifikaten. Diese Unterstützungsfunktion bietet auch einen höheren Sicherheitsstandard und die Möglichkeit zur Übertragung umfangreicherer Nachrichten.

LDAP-Protokoll

Das IBM Directory unterstützt LDAP (Lightweight Directory Access Protocol), um Anwendungen den Zugriff auf seine zentralen Serverdienste zu ermöglichen. LDAP ist ein Protokoll, das auf dem X.500-Standard basiert. Es wird über TCP/IP ausgeführt und steuert den Verzeichniszugriff durch die Verwendung von registrierten Namen (DNs) und Kennwörtern. Da LDAP SSL-Verbindungen unterstützt, können über dieses Protokoll auch Nachrichten verschlüsselt und Clients und Server gegenseitig authentifiziert werden.

Bei Tivoli PKI verwendet der RA-Server LDAP für die Kommunikation mit dem Directroy-Server. Die RA publiziert Zertifikate, Zertifikatswiderrufslisten sowie andere Informationen zu registrierten Entitäten und Zertifizierungsregeln in regelmäßigen Abständen im Directory.

Im aktuellen Release von Tivoli PKI wird die Kompatibilität mit den Objektklassen und Schemata von LDAP Version 3 unterstützt. Bereits vorhandene Tivoli PKI-Anwendungen, die mit Schemata von PKIX LDAP Version 2 arbeiten, können vorhandene Schemata und Objektklassen weiterhin nutzen.

Objektspeicher

Jede Tivoli PKI-Komponente verfügt über einen Objektspeicher. Beim Objektspeicher handelt es sich um ein auf einer Platteneinheit angelegtes Repository für permanente Objekte. Es dient zum Speichern von momentan ausgeführten Transaktionen sowie Statusinformationen zu diesen Transaktionen. Bei den Objekten kann es sich um aktive Steuerobjekte (z. B. Zertifikate, Anforderungen und CRLs) oder um Ersatzobjekte handeln. Als Ersatzobjekt bezeichnet man einen Bereich, in dem Statusinformationen zu dem zugehörigen Objekt gespeichert werden.

Da Objekte im Objektspeicher im ASN.1-Format gespeichert werden, ist das Abrufen und Speichern relativ aufwendig. Der Objektspeicher speichert Änderungen an den Objekten im Cache und aktualisiert den Plattenspeicher erst dann, wenn sich der Objektstatus ändert oder das Objekt durch eine Benutzerschnittstelle geändert wird.

Um den Aufwand durch die ASN.1-Syntaxanalyse so gering wie möglich zu halten, verwendet Tivoli PKI für den Objektspeicher eine übergeordnete Objekt-Cache-Schicht, über die die im Objektspeicher gespeicherten Objekte im Durchschreibmodus übergeben werden können. Hierdurch wird die Syntaxanalyse eines Objekts nur dann erforderlich, wenn zum ersten Mal nach dem Serverneustart auf dieses verwiesen wird.

Die Objekt-Cache-Schicht bietet einen zusätzlichen Speicherbereich für Objekte, der keinen Plattenspeicherplatz belegt. Tivoli PKI verwendet diesen Bereich zum Speichern temporärer, sicherheitsrelevanter Daten wie z. B. des Kennworts, durch das ein Vorabregistrierungssatz geschützt wird. Der Objekt-Cache kann auch zum Sperren von Datensatzobjekten verwendet werden, um den gleichzeitigen Zugriff durch mehrere Threads zu verhindern.

Trust-Modell

Die Sicherheit in einem Tivoli PKI-System wird durch die Code- und Nachrichtenunterzeichnung, die Datenverschlüsselung sowie das sichere Speichern von Schlüsseln und Kennwörtern gewährleistet.

Codeunterzeichnung

Der Hauptcode von Tivoli PKI wird bei der Herstellung unterzeichnet. Wenn der Code werksseitig mit einem privaten Schlüssel unterzeichnet wird, wird er als statisches, geschütztes Objekt definiert. Er kann nicht geändert oder ersetzt werden, ohne dass dies festgestellt werden kann. Andere Codeobjekte können den entsprechenden öffentlichen Schlüssel und die interne Prüfbibliothek verwenden, um die Kommunikation zu authentifizieren, bevor ein Datenaustausch stattfindet.

Nachrichtenunterzeichnung

Um noch weiter reichende Authentifizierungsservices zur Verfügung zu stellen, werden durch den Konfigurationsprozess Unterschriftsschlüssel für den RA-, CA- und Prüfserver generiert. Hierdurch kann sichergestellt werden, dass alle Kommunikationsoperationen zwischen den einzelnen Komponenten nur mit einer entsprechenden Unterschrift ausgeführt werden können. So können beispielsweise

alle Nachrichten, die zwischen der RA und dem CA ausgetauscht werden, auf der Basis der Unterschrift der jeweiligen Komponente authentifiziert werden.

Datenverschlüsselung

Alle in Schlüsselspeichern (KeyStores) gespeicherten Informationen werden verschlüsselt. Darüber hinaus verschlüsselt DB2 einen Großteil der Informationen, die in den Tivoli PKI-Datenbanken gespeichert werden.

Schlüsselspeicher (KeyStores)

Tivoli PKI stellt Unterstützung für Schlüsselspeicher (KeyStores) zur Verfügung. Hierbei handelt es sich um sichere Bereiche, in denen private Schlüssel, Zertifikate, Nachrichtenauthentifizierungscodes (MAC) und andere sicherheitsrelevante Objekte gespeichert werden. Für die CA- und Prüfkomponenten sowie für eine Reihe von Server-Agenten, die die Ausführung von Server-Transaktionen unterstützen, sind verschiedene Schlüsselspeicher vorhanden. Die Informationen in den einzelnen Schlüsselspeichern werden verschlüsselt, so dass der Zugriff ausschließlich über ein Kennwort möglich ist, das für den jeweiligen Schlüsselspeicher definiert wird.

Dieses Sicherheitsmodell trägt zur Gewährleistung der Systemintegrität bei, indem es Objekte schützt, die im Schlüsselspeicher gespeichert sind. Darüber hinaus stellt dieses Modell die Vertraulichkeit dieser Objekte sicher, indem es ausschließlich gesicherten Systemkomponenten - d. h. Systemkomponenten, die werksseitig mit einem Schlüssel unterzeichnet wurden - den Zugriff auf die Schlüsselspeicher und die darin gespeicherten verschlüsselten Daten gewährt.

Während der Konfiguration werden zwei Kennwörter definiert. Hierbei handelt es sich um das cfguser- und das Steuerprogrammkennwort. Diese Kennwörter können identisch sein oder voneinander abweichen. Nach der Konfiguration muss für jeden Schlüsselspeicher ein eindeutiges Kennwort definiert werden. Informationen zum Durchführen dieser Änderungen mit dem Dienstprogramm für die Kennwortänderung (Change Password) finden Sie im Handbuch *Tivoli PKI Systemverwaltung*.

Unterstützte Standards

Tivoli Public Key Infrastructure unterstützt die folgenden Standards für die Verschlüsselung mit öffentlichen Schlüsseln:

Komponente	Standard
Registrierungs-stelle	■ Secure Sockets Layer (SSL) Version 2 und Version 3 mit Client-Authentifizierung ■ PKCS #10-Format für Browser- und Server-Zertifikate mit einer Base64-codierten PKCS #7-Antwort ■ PKIX CMP-Zertifikatsformat mit einer PKIX CMP-Antwort ■ IPSec-Zertifikatsformat ■ S/MIME-Zertifikatsformat ■ Browser-Zertifikate für: • Microsoft Internet Explorer Versionen 4.x und 5.x • Netscape Navigator und Netscape Communicator Version 6.x ■ Server-Zertifikate für: • Netscape Enterprise Server • Microsoft Internet Information Server ■ Smart-Card-Zertifikate (PKCS #11-Schnittstelle) für Netscape Navigator und Netscape Communicator Version 6.x ■ LDAP-Standard für die Kommunikation mit dem Directory ■ PKIX CMP via TCP/IP für die Kommunikation mit dem Zertifikats-aussteller
Zertifikats-aussteller	■ X.509v3-Zertifikate ■ Zertifikatswiderrufslisten (CRLv2) ■ Schlüssellängen von bis zu 1024 Bit für die Verschlüsselung und Schlüssel für den Schlüsselaustausch ■ Schlüssellängen von bis zu 2048 Bit für CA-Unterschriftsschlüssel ■ RSA-Algorithmen für die Verschlüsselung und die Unterzeichnung ■ MD5- und SHA-1-Hash-Algorithmen ■ PKIX CMP via TCP/IP für die Kommunikation mit der Registrierungsstelle
IBM Directory	LDAP Version 3.2 mit RFC 1779-Syntax

Komponente	Standard
IBM 4758 PCI Cryptographic Coprocessor (Hardware)	■ FIPS 140 Stufe 4-Anforderungen für den Schutz gegen physische Beschädigung ■ Unterstützung für branchenübliche Verschlüsselungsstandards: • DES für die Verschlüsselung und Entschlüsselung • RSA für die Unterzeichnung und Unterschriftsprüfung • PKCS #1-Blocktyp 00 • PKCS #1-Blocktyp 01 • PKCS #1-Blocktyp 02 • MD5- und SHA-1-Hash-Algorithmen • X9.9 und X9.23 ANSI • ISO 9796
IBM CCA Cryptographic Coprocessor Support Program	Dieses Unterstützungsprogramm stellt Services für den IBM 4758 PCI Cryptographic Coprocessor zur Verfügung, einschließlich der sicheren Generierung von RSA-Schlüsselpaaren mit Modulus-Längen bis zu 2048 Bit sowie folgenden Funktionen: ■ SET (Secure Electronic Transaction) ■ DES für die Verschlüsselung und Entschlüsselung ■ RSA für die Unterzeichnung und Unterschriftsprüfung ■ MD5- und SHA-1-Hash-Algorithmen

Zertifikate gemäß X.509 Version 3

Tivoli PKI-Zertifikate unterstützen die meisten Felder und Erweiterungen, die im Standard X.509 Version 3 (X.509v3) definiert sind. Durch diese Unterstützung können die Zertifikate für die meisten Verschlüsselungsoperationen verwendet werden, wie beispielsweise SSL, IPSec, VPN und S/MIME.

Tivoli PKI-Zertifikate können die folgenden Erweiterungstypen enthalten:

Standarderweiterungen

Die Standard-X.509v3-Zertifikatserweiterungen, z. B. Schlüsselverwendung, Verwendungszeitraum privater Schlüssel, Alternativname des Zertifikatsgegenstands, Basiseinschränkungen und Namenseinschränkungen.

Allgemeine Erweiterungen

Erweiterungen, die ausschließlich bei Tivoli PKI vorhanden sind, wie beispielsweise die Host-Identitätszuordnung. Diese Erweiterung ordnet den Zertifikatsgegenstand einer entsprechenden Identität auf einem Host-System zu.

Private Erweiterungen

Erweiterungen, die eine Anwendung dazu verwenden kann, einen Online-Prüfservice zu identifizieren, der den ausstellenden CA unterstützt.

Zur Unterstützung der Registrierungsregeln des jeweiligen Unternehmens bietet Tivoli PKI auch die Möglichkeit, die Zertifikatserweiterungen anzupassen und zu definieren. So können Sie beispielsweise die Erweiterungen, die in den Standardzertifikatsprofilen angegeben sind, ändern oder Profile erstellen, die Zertifikate mit anderen Erweiterungen zurückgeben.

Umfassende Informationen zum Erstellen und Anpassen von Zertifikatserweiterungen und Zertifikatsprofilen finden Sie im Handbuch *Tivoli PKI Anpassung*.

2

Systemvoraussetzungen

Die verwendete Betriebsumgebung muss die Software- und Hardwarevoraussetzungen erfüllen, die in den folgenden Abschnitten erläutert werden. Die neuesten Informationen zu den Systemvoraussetzungen finden Sie in den Release-Informationen zu Tivoli Public Key Infrastructure (PKI). Diese Datei kann Informationen enthalten, die die entsprechenden Angaben in den Produktveröffentlichungen ersetzen.

Die aktuellste Version dieses Dokuments können Sie über die Website von Tivoli Public Key Infrastructure abrufen.

Softwarevoraussetzungen für den Server

Um die Arbeitsbelastung auf mehrere Prozessoren zu verteilen und die vorhandene Systemkonfiguration in Ihrem Unternehmen zu unterstützen, können Sie die Tivoli PKI-Server-Programme auf mehreren Maschinen installieren. Eine Erläuterung zu den unterschiedlichen Möglichkeiten, Tivoli PKI in der jeweiligen Umgebung zu installieren, finden Sie im Abschnitt „Unterstützte Serverkonfigurationen” auf Seite 53.

In der folgenden Tabelle sind die Betriebssystem- und Softwarevoraussetzungen für Tivoli PKI aufgeführt.

Produkt	Anmerkungen
Eines der folgenden Betriebssysteme: ■ IBM AIX/6000 (AIX), Version 4.3.3 Wartungsstufe 6 ■ Microsoft Windows NT, Version 4.0 mit Service Pack 5	■ Erforderlich. ■ Alle Tivoli PKI-Server-Programme müssen auf derselben Plattform installiert werden. AIX- und Windows NT-Maschinen dürfen nicht gleichzeitig in derselben Tivoli PKI-Installation verwendet werden.
IBM DB2 Universal Database, Version 6.1 Fix Pack 4	■ Erforderlich; im Tivoli PKI-Datenträgerpaket enthalten. ■ Für jede Tivoli PKI-Server-Komponente ist eine eindeutige Datenbank vorhanden. Vor der Installation von Tivoli PKI muss DB2 auf jeder Maschine installiert werden, die als Tivoli PKI-Server verwendet werden soll.
IBM WebSphere Application Server, Standard Edition, Version 3.5 Program Temporary Fix (PTF) 4. Dieses Produkt umfasst IBM HTTP Server, Version 1.3.12.3 und Sun Java Development Kit (JDK), Version 1.2.2 Program Temporary Fix (PTF) 8	■ Erforderlich; im Tivoli PKI-Datenträgerpaket enthalten. ■ Vor der Installation von Tivoli PKI muss die Web-Server-Software auf derselben Maschine installiert werden, auf der auch die Registrierungsstelle installiert werden soll.
IBM Directory, Version 3.1.1.5	■ Erforderlich; im Tivoli PKI-Datenträgerpaket enthalten. ■ Vor der Installation von Tivoli PKI muss die Directory-Software installiert werden. Die Directory-Software kann auf derselben Maschine wie Tivoli PKI oder auf einer fernen Maschine installiert werden.

Produkt	Anmerkungen
■ IBM 4758 PCI Cryptographic Coprocessor ■ IBM 4758 CCA Support Program, Version 2.2.1.0	■ Optional und lediglich für AIX-Systeme verfügbar. Dieses Produkt muss über die üblichen IBM Vertriebskanäle bestellt werden. ■ Vor der Installation von Tivoli PKI müssen der IBM 4758 PCI Cryptographic Coprocessor und das zugehörige Unterstützungsprogramm auf dem Server installiert werden, auf dem der Zertifikatsaussteller und die Registrierungsstelle installiert werden sollen. ■ Für die Verschlüsselungskarte der Einheit IBM 4758 ist ein PCI-Bus auf dem RS/6000-System erforderlich.

Hardwarevoraussetzungen für den Server

Die Maschinenkonfiguration, die Sie für Tivoli PKI verwenden, ist abhängig von der erwarteten Geschäftsaktivität und davon, ob Tivoli PKI unter AIX oder Windows NT verwendet werden soll.

- Wenn Sie Tivoli PKI auf einem AIX-System ausführen möchten, müssen Sie das Produkt auf einer IBM RISC System/6000-Maschine (RS/6000®) installieren.
- Wenn Sie Tivoli PKI auf einem Windows NT-System ausführen wollen, empfiehlt IBM, das Produkt auf einem IBM Netfinity®-Server zu installieren.

Verwenden Sie die folgenden Definitionen als Richtlinie für die Berechnung der Kapazitäts- und Durchsatzanforderungen:

Kleine Produktions- oder Testumgebung
Ein Standort, an dem Hunderte von Zertifikaten pro Tag ausgestellt werden. Dabei kann es sich um ein System handeln, das für die Ausstellung von Zertifikaten an Mitarbeiter über ein Intranet eingerichtet wird, oder um ein System, das zu Testzwecken oder zur Anwendungsentwicklung konfiguriert ist.

Mittlere Produktionsumgebung
Ein Standort, an dem Tausende von Zertifikaten pro Tag ausgestellt werden. Dabei kann es sich um ein System handeln, das von kleinen und mittleren Unternehmen eingerichtet wird, um Zertifikate über das Internet auszustellen.

Große Produktionsumgebung
Ein Standort, an dem Tausende von Zertifikaten pro Tag ausgestellt werden. Dabei kann es sich um ein System handeln, das von einem großen Unternehmen für die Ausstellung von Zertifikaten über das Internet eingerichtet wird. Es kann sich auch um ein System handeln, das als unabhängiger Dritter CA-Services für andere Unternehmen zur Verfügung stellt.

Die folgende Tabelle enthält eine Übersicht zu den Mindesthardwarevoraussetzungen in einer kleinen Produktionsumgebung. Sie sollten die Konfiguration der physischen Maschinen an die erwarteten Verarbeitungsanforderungen anpassen.

Plattform	Maschinentyp	Prozessoren	Plattenspeicherplatz	Hauptspeicher
AIX	RS/6000	1 (233 MHz)	4 GB	256 MB
NT	PC	1 (Intel Pentium 300 MHz)	2 GB	256 MB

Voraussetzungen für den Setup Wizard

IBM empfiehlt für die Ausführung des Konfigurations-Applets von Tivoli PKI (Setup Wizard) die folgende Workstation-Konfiguration.

- Folgende physische Maschinenkonfiguration:
  - Intel Pentium-Prozessor mit mindestens 64 MB Arbeitsspeicher
  - Ein Computerbildschirm, der Auflösungen von 1024 x 768 oder höher mit 65536 Farben unterstützt
- Eines der folgenden Betriebssysteme:
  - Microsoft Windows 95
  - Microsoft Windows 98
  - Microsoft Windows NT
- Ein Webbrowser, der Applets auf der Basis von JDK 1.1 unterstützt, z. B. die nachfolgend aufgeführten Webbrowser:
  - Netscape Navigator oder Netscape Communicator, nur Version 4.7*x*.

    Anmerkung: Netscape Navigator oder Netscape Communicator, Version 6 wird für das Konfigurations-Applet oder RA Desktop nicht unterstützt. Netscape Navigator oder Netscape Communicator, Version 6 wird nur bei der Ausführung von Zertifikatsoperationen wie z. B. dem Registrieren, Erneuern und Widerrufen sowie bei der Sicherung und Wiederherstellung unterstützt.
  - Microsoft Internet Explorer, ab Version 5.0

  Sie müssen die offizielle, von Netscape oder Microsoft vertriebene Version des Browsers installieren. Bei Versionen anderer Lieferanten werden Informationen möglicherweise nicht korrekt angezeigt, vor allem dann, wenn nicht die englische Version des Applets ausgeführt wird.

Umfassende Informationen zum Ausführen des Setup Wizard und zur Konfiguration des Tivoli PKI-Systems finden Sie im Handbuch *Tivoli PKI Konfiguration*.

Client-Voraussetzungen

Informationen dazu, ob Ihre Workstation die Anforderungen zum Einsatz eines Browsers für die Anforderung und Verwaltung von Zertifikaten erfüllt, finden Sie im *Tivoli PKI Benutzerhandbuch*.

Informationen dazu, ob Ihre Workstation die Anforderungen zur Ausführung von Tivoli PKI RA Desktop erfüllt, finden Sie im Handbuch *Tivoli PKI RA Desktop*.

3

Tivoli PKI - Planung

Das vorliegende Kapitel enthält Informationen zur interaktiven Kommunikation von Tivoli Public Key Infrastructure mit den Programmen, die für den Betrieb des Systems erforderlich sind. Vor der Installation der verschiedenen Softwareprodukte oder der Konfiguration des Systems sollten Sie die Prüfliste im Abschnitt „Prüfliste für die Installationsplanung" auf Seite 34 durcharbeiten. Nachdem Sie sich vergewissert haben, dass alle in dieser Prüfliste aufgeführten Voraussetzungen erfüllt sind, sollten Sie die restlichen Abschnitte dieses Kapitels lesen. Es enthält auch Richtlinien zur Vorbereitung der Betriebsumgebung für den Einsatz von Tivoli PKI und behandelt die folgenden Themen:

- Vorgehensweise zum physischen Sichern des Systems und zum Schutz des Systems gegen unbefugten elektronischen Zugriff.
- Vorgehensweise zum Konfigurieren von IP-Aliasnamen für den Web-Server zum Unterstützen der Firewall-Anforderungen Ihres Unternehmens.
- Vorgehensweise von Tivoli PKI zum Erstellen und Verwenden von Datenbanken.
- Vorgehensweise von Tivoli PKI zur Interaktion mit dem Directory.
- Vorgehensweise von Tivoli PKI zur Interaktion mit dem IBM 4758 PCI Cryptographic Coprocessor.
- Vorgehensweise von Tivoli PKI zur Interaktion mit Policy Director.

- Empfohlene Server-Konfigurationen zur Ausführung von Tivoli PKI in einer Umgebung mit mehreren Maschinen.
- Überlegungen zur Landessprache zur Ausführung von Tivoli PKI mit den länderspezifischen Angaben Ihres Unternehmens.
- Übersicht zu den CDs, die im Tivoli PKI-Produktverteilerpaket enthalten sind.

Prüfliste für die Installationsplanung

In der folgenden Prüfliste sind die Voraussetzungen aufgeführt, die zur erfolgreichen Ausführung der Tivoli PKI-Installation erfüllt werden müssen. Prüfen Sie diese Voraussetzungen und markieren Sie diese mit einem Haken (✓), nachdem Sie sie erfüllt haben.

Voraussetzung	Beschreibung	Kommentare	Erfüllt? ✓
Produktspezifische Schulung	Tivoli PKI	Weitere Einzelheiten erfahren Sie vom zuständigen IBM oder Tivoli-Ansprechpartner.	
	IBM 4758 PCI Cryptographic Coprocessor	Weitere Einzelheiten erfahren Sie vom zuständigen IBM oder Tivoli-Ansprechpartner.	

Voraussetzung	Beschreibung	Kommentare	Erfüllt? ✓
Softwarevoraussetzungen für den Server	Eines der folgenden Betriebssysteme: ■ IBM AIX/6000 (AIX), Version 4.3.3 Wartungsstufe 6 ■ Microsoft Windows NT, Version 4.0 mit Service Pack 5		
	IBM DB2 Universal Database Version 6.1 Fix Pack 4	Erforderlich; im Tivoli PKI-Datenträgerpaket enthalten.	
	IBM WebSphere Application Server, Standard Edition Version 3.5 Program Temporary Fix 4. Dieses Produkt umfasst IBM HTTP Server Version 1.3.12.3 und Sun Java Development Kit (JDK) Version 1.2.2 Program Temporary Fix (PTF) 8.	Erforderlich; im Tivoli PKI-Datenträgerpaket enthalten.	
	IBM Directory Version 3.1.1.5	Erforderlich; im Tivoli PKI-Datenträgerpaket enthalten.	
	IBM Global Security Kit SSL Runtime Toolkit (GSKit) Version 4.0.3.116	Erforderlich; im Tivoli PKI-Datenträgerpaket enthalten.	
	IBM KeyWorks Version 1.1.3.1	Erforderlich; im Tivoli PKI-Datenträgerpaket enthalten.	
	■ IBM 4758 PCI Cryptographic Coprocessor ■ IBM 4758 CCA Support Program, Version 2.2.1.0.	Optional und lediglich für AIX-Systeme verfügbar. Dieses Produkt muss über die üblichen IBM Vertriebskanäle bestellt werden.	

Voraussetzung	Beschreibung	Kommentare	Erfüllt? ✓
Hardwarevoraussetzungen für den Server	Eine der folgenden Plattformen: ■ AIX: IBM RISC System/6000 ■ Windows NT: IBM Netfinity-Server		
	■ 4 GB Plattenspeicherplatz ■ 256 MB Hauptspeicher ■ Ein 233-MHz-Prozessor (AIX) oder ■ ein 300-MHz-Intel Pentium-Prozessor (Windows NT)		

Voraussetzung	Beschreibung	Kommentare	Erfüllt? ✓
Voraussetzungen für den Setup Wizard	■ Intel Pentium-Prozessor mit mindestens 64 MB Arbeitsspeicher ■ Ein Computerbildschirm, der Auflösungen von 1024 x 768 oder höher mit 65536 Farben unterstützt		
	Eines der folgenden Betriebssysteme: ■ Microsoft Windows 95 ■ Microsoft Windows 98 ■ Microsoft Windows NT		
	Ein Webbrowser, der Applets auf der Basis von JDK 1.1 unterstützt, z. B. die nachfolgend aufgeführten Webbrowser: ■ Netscape Navigator oder Netscape Communicator, Version 4.7x (nur für Windows-Plattformen) ■ Microsoft Internet Explorer, ab Version 5.0	Sie müssen die offizielle, von Netscape oder Microsoft vertriebene Version des Browsers installieren. Bei Versionen anderer Lieferanten werden Informationen möglicherweise nicht korrekt angezeigt, vor allem dann, wenn nicht die englische Version des Applets ausgeführt wird.	

Voraussetzung	Beschreibung	Kommentare	Erfüllt? ✓
Voraussetzungen für RA Desktop	■ Intel Pentium-Prozessor mit mindestens 64 MB Arbeitsspeicher ■ Ein Computerbildschirm, der Auflösungen von 1024 x 768 oder höher mit 65536 Farben unterstützt		
	Eines der folgenden Betriebssysteme: ■ Microsoft Windows 95 ■ Microsoft Windows 98 ■ Microsoft Windows NT		
	Einer der folgenden Webbrowser: ■ Netscape Navigator oder Netscape Communicator, nur Release 4.7*x* ■ Microsoft Internet Explorer, ab Release 5.0	Sie müssen die offizielle, von Netscape oder Microsoft bereitgestellte Version des Browsers installieren. Für den Internet Explorer müssen Sie über Java Virtual Machine (JVM), Release 5.00, ab Build 3167 verfügen.	

Voraussetzung	Beschreibung	Kommentare	Erfüllt? ✓
Client-Voraussetzungen	■ Intel Pentium-Prozessor mit mindestens 64 MB Arbeitsspeicher Darüber hinaus ist Folgendes erforderlich: ■ Ein Computerbildschirm, der Auflösungen von 1024 x 768 oder höher mit 65536 Farben unterstützt		
	Eines der folgenden Betriebssysteme: ■ Microsoft Windows 95 ■ Microsoft Windows 98 ■ Microsoft Windows NT		
	Ein Webbrowser wie z. B. die folgenden Produkte: ■ Netscape Navigator oder Netscape Communicator, ab Version 4.7 für Windows-Plattformen ■ Microsoft Internet Explorer, ab Version 5.0	Sie müssen die offizielle, von Netscape oder Microsoft bereitgestellte Version des Browsers installieren.	

System sichern

Tivoli PKI verwendet die Verschlüsselung, digitale Unterschriften und digitale Zertifikate, um Transaktionen zu schützen und Ihre Ressourcen gegen unberechtigten Zugriff zu sichern. Die Sicherheit des Tivoli PKI-Servers ist jedoch abhängig von der Sicherheit der zugrundeliegenden Betriebsumgebung.

Dieser Abschnitt enthält Vorschläge zur Sicherung der physischen Umgebung des Systems, um die Möglichkeit unbefugten Zugriffs auf ein Minimum zu reduzieren, bevor Sie mit der Installation der Tivoli PKI-Software beginnen.

Im Folgenden sind einige Faktoren aufgeführt, die bei der Sicherung des Systems berücksichtigt werden sollten:

Isolierter Bereich

Richten Sie den Server in einem isolierten Raum ein, der ausschließlich CA-Aktivitäten dient. Wenn möglich, sollte der Raum über verstärkte Wände, eine einzige Massivholz- oder -stahltür und eine stabile Decke ohne herausnehmbare Elemente verfügen. Darüber hinaus sollte der Raum über einen doppelten Boden zum Schutz gegen Entladungen im Falle eines Feuers verfügen.

Verwalteter Bereich

Der Raum sollte über eine unterbrechungsfreie Stromversorgung (UPS) verfügen, die von den Computern, der Beleuchtung, den Bewegungsmeldern sowie den Heizungs- und Kühlungssystemen verwendet wird. Überwachen Sie die Temperatursteuerung, um sicherzustellen, dass die Belüftung ausreicht, um die von den Geräten erzeugte Wärme auszugleichen.

Zugangskontrolle

Der Zugang zum Serverbereich kann auf unterschiedliche Weise kontrolliert werden, beispielsweise durch Ausweise oder durch Türschlösser, für die Zugangscodes über eine Tastatur eingegeben werden müssen. Um die Manipulation durch eine einzelne Person zu verhindern, sollten Kontrollen eingerichtet werden, bei denen von mindestens zwei vertrau-

enswürdigen Mitarbeitern die entsprechenden Identitätsnachweise vorgelegt werden müssen.

Darüber hinaus sollten Sie den Raum überwachen, um zu protokollieren, wann jemand den Sicherheitsbereich betritt und um wen es sich handelt. Maximale Sicherheit kann durch die Installation von Bewegungsmeldern innerhalb des Raumes und vor der Tür erreicht werden.

Kommunikationskontrolle

Am Tivoli PKI-Server sollten keine freien, aktiven Anschlüsse zur Verfügung stehen. Konfigurieren Sie das System so, dass es nur an den Anschlüssen auf Anforderungen wartet, die explizit aktiven Tivoli PKI-Anwendungen zugeordnet sind.

Firewall-Techniken verwenden

IBM empfiehlt dringend die Installation einer Firewall, wie beispielsweise IBM Firewall, um das Tivoli PKI-System gegen unbefugten Zugriff über einen anderen Teil des Netzes zu schützen. Eine Firewall bietet die folgenden Möglichkeiten für den Schutz des Systems:

- Steuerung der Anwendungen, die via Internet auf das interne Netz zugreifen können.
- Steuerung der Adressen im internen Netz, auf die eine berechtigte Anwendung zugreifen kann.
- Verhinderung des Zugriffs interner Anwendungen auf das externe Netz (Internet).
- Authentifizierung der Identität der Quellen für alle eingehenden Anforderungen und Genehmigung bzw. Verweigerung des Zugriffs auf der Basis der Prüfungsergebnisse.

Um die Zugriffseinschränkungen umzusetzen, müssen die Tivoli PKI-Server hinter der Firewall konfiguriert werden. Die installierte Firewall muss mindestens die folgenden Funktionen zur Verfügung stellen:

- Einen Überwachungs-Router, mit dem Datenpakete den in Ihrem Unternehmen gültigen Regeln entsprechend selektiv geblockt werden können. So sollte es die Firewall beispielsweise ermögli-

chen, Steuerfunktionen einzurichten, mit denen die Kommunikation auf bestimmte IP-Adressen und Anschlüsse begrenzt werden kann.

- Einen Proxy-Server, der als Vermittler zwischen Client/Server-Anforderungen eingesetzt werden kann. So sollte es die Firewall beispielsweise ermöglichen, FTP- oder HTTP-Anforderungen von Benutzern abzufangen, bevor sie an den entsprechenden Server-Prozess weitergeleitet werden. Auf diese Weise wird die direkte Kommunikation zwischen dem Client und dem Server verhindert.
- Ein Peripherienetz, das einen zusätzlichen Puffer bietet, der das interne Netz abschirmen und schützen kann, falls im externen Netz ein Fehler auftritt.

Bitte beachten Sie, dass Sie die Tivoli PKI-Serverprogramme auf mehreren Maschinen installieren können; dieses Konzept bietet eine Reihe von Vorteilen. So können Sie beispielsweise die Leistung verbessern, indem Sie die Arbeitsmenge auf mehrere Prozessoren verteilen, separate Datensicherungszeitpläne definieren und den Zugriff auf verschiedene Prozesse über die IP-Adressenzuordnung steuern. Um die Sicherheit für diese Programme sicherzustellen, müssen diese Server hinter der Firewall konfiguriert werden. Wenden Sie dieselben Vorsichtsmaßnahmen an, die Sie auch für den Hauptserver implementiert haben.

Mit Tivoli PKI-Datenbanken arbeiten

Tivoli PKI verwendet zum Verwalten von Daten IBM DB2 Universal Database. Die im Paket mit den Tivoli PKI-Datenträgern enthaltene DB2-Version wird ausschließlich für die Verwendung durch Tivoli PKI-Anwendungen zur Verfügung gestellt. Wenn Sie die Datenbanksoftware anpassen oder zusammen mit anderen Anwendungen als Tivoli PKI verwenden wollen, müssen Sie eine Lizenz für eine Vollversion von IBM DB2 Enterprise Edition kaufen.

Wenn Sie Tivoli PKI in einer Konfiguration mit mehreren Maschinen installieren wollen, müssen Sie auf allen Maschinen, auf denen eine

Serverkomponente von Tivoli PKI installiert werden soll, zuerst die Tivoli PKI-Datenbanksoftware installieren.

Im Rahmen der Ausführung eines Konfigurationsprogramms für den Installationsabschluss erstellt Tivoli PKI die Datenbank 'cfgdb' für Konfigurationsdaten und füllt sie mit Standardkonfigurationswerten.

Während der Konfiguration erstellt Tivoli PKI die folgenden Datenbanken für CA-, Registrierungs- und Prüfdaten sowie für Daten zur Schlüsselsicherung und -wiederherstellung. Wenn Sie Tivoli PKI unter AIX installieren, müssen Sie Plattenpartitionen für diese Datenbanken erstellen, bevor Sie den Installationsprozess starten. Der Abschnitt „AIX-Datenträgergruppen und -Dateisysteme konfigurieren" auf Seite 61 enthält Einzelheiten hierzu.

- ibmdb
- pkrfdb
- adtdb
- krbdb

Darüber hinaus erstellt Tivoli PKI die Datenbank 'ldapdb' für das Directory, falls diese nicht bereits vorhanden ist:

Wenn Sie alle Serverkomponenten auf derselben Maschine installieren, erstellen die Konfigurationsprogramme die Datenbanken im Hintergrund. Wenn Sie die CA-, Prüf- oder Directory-Komponente auf fernen Maschinen installieren, müssen Sie während der Konfiguration bestimmte Schritte ausführen, um sicherzustellen, dass die Exemplare für die Datenbanken korrekt erstellt werden. Erläuterungen zu diesen fernen Konfigurationsprozeduren finden Sie im Handbuch *Tivoli PKI Konfiguration*.

Wenn Sie Tivoli PKI unter AIX installieren, werden die Konfigurations-, CA-, Registrierungs- und Prüfdatenbank sowie die Datenbank für die Schlüsselsicherung und -wiederherstellung unter dem Exemplar 'cfguser' erstellt. Wenn noch keine Datenbank für das Directory erstellt wurde, wird diese ebenfalls unter dem Exemplar mit dem Namen 'cfguser' generiert.

Bei der Installation von Tivoli PKI unter Windows NT entspricht der Exemplarname für die Tivoli PKI-Datenbanken dem Benutzernamen, unter dem Sie das Produkt installieren. (Der empfohlene Wert lautet 'cfguser', in Ihrer Installation wurde jedoch möglicherweise ein anderer Wert gewählt.) Wenn noch keine Datenbank für das Directory erstellt wurde, wird diese unter dem Exemplar mit dem Namen 'ldapInst' generiert.

Zur Unterstützung von Sicherungs- und Wiederherstellungsoperationen ermöglicht Tivoli PKI die Erstellung von Prüfprotokollen für Registrierungs- und Zertifizierungsereignisse. Das Handbuch *Tivoli PKI Systemverwaltung* enthält Richtlinien zur Archivierung der Prüfprotokolle sowie zum Sichern und Zurückschreiben des Systems. Zusätzliche Informationen zum Sichern und Zurückschreiben der Datenbanken erhalten Sie beim zuständigen DB2-Datenbankadministrator.

IP-Aliasnamen für den Webserver konfigurieren

Das Datenträgerpaket von Tivoli Public Key Infrastructure enthält die für Tivoli PKI erforderliche Web-Server-Software: IBM WebSphere Application Server, IBM HTTP Server sowie Sun Java Development Kit (JDK). Nach der Installation dieser Software können Sie bestimmte Ports für die Verarbeitung öffentlicher und gesicherter Anforderungen konfigurieren.

In einem Tivoli PKI-System muss der Webserver die folgenden Anforderungstypen unterstützen:

- Nicht-SSL-Anforderungen (SSL = Secure Sockets Layer) oder öffentliche Anforderungen
- Sichere SSL-Anforderungen ohne Client-Authentifizierung
- Sichere SSL-Anforderungen mit Client-Authentifizierung

In der Standardkonfiguration ordnet Tivoli PKI Ports auf dem Web-Server zu, die zur Verarbeitung der verschiedenen Anforderungsarten dienen. Auf diese Weise können Sie das System so verwenden, wie es installiert wurde, ohne spezielle Anpassungen an Ihrer Netzkonfiguration vorzunehmen.

Die folgende Tabelle enthält eine Übersicht zu dieser Architektur und den für die Ports verwendeten Standardwerten:

Protokoll	SSL	Server-Authentifizierung	Client-Authentifizierung	Anschlussnummer
HTTP	Nein	Nein	Nein	80
HTTPS	Ja	Ja	Nein	443
HTTPS	Ja	Ja	Ja	1443

In vielen gesicherten Systemen können nur die Ports 80 und 443 über die Firewall geöffnet sein und nur der Port 443 kann für die Herstellung von SSL-Verbindungen genutzt werden. Wenn dies auch auf Ihr Unternehmen zutrifft, müssen Sie den Webserver so konfigurieren, dass die unterschiedlichen Anforderungstypen über denselben Port verarbeitet werden können. Das System kann beispielsweise so konfiguriert werden, dass die beiden sicheren Server am Port 443 Anforderungen empfangen.

Um für eine einzelne Maschine mehrere Zugriffspunkte über denselben Port bereitzustellen, müssen Namen für virtuelle Hosts definiert und diese Namen IP-Adressen zugeordnet werden, bei denen es sich um Aliasnamen der tatsächlichen IP-Adresse der Maschine handelt. Dieses Konzept, das als IP-Aliasnamenumsetzung bezeichnet wird, ermöglicht es, mehrere unabhängige Server auf einer einzelnen Maschine auszuführen.

Anmerkung: Wenn Sie nicht beabsichtigen, die Standardkonfigurationswerte für Web-Server-Ports zu verwenden, müssen Sie die IP-Aliasnamen konfigurieren, **bevor** Sie das Konfigurations-Applet von Tivoli PKI ausführen. Die Konfigurationsprogramme verwenden diese Werte bei der Erstellung des CA-Zertifikats für Ihr System.

IP-Aliasnamen werden in TCP/IP DNS (Domain Name Services = Domänennamenservices) definiert. Gehen Sie unter Tivoli PKI folgendermaßen vor, um zwei Aliasnamen zu konfigurieren:

- Konfigurieren Sie DNS und geben Sie den Host-Namen und die IP-Adresse der Maschine an. Verwenden Sie diesen Eintrag für den öffentlichen Server, der Nicht-SSL-Anforderungen am Anschluss 80 empfängt.
- Fügen Sie einen (virtuellen) Host-Aliasnamen und eine IP-Aliasadresse hinzu. Verwenden Sie diesen Eintrag für den sicheren Web-Server, der SSL-Anforderungen ohne Client-Authentifizierung am Anschluss 443 empfängt.
- Fügen Sie einen zweiten Host-Aliasnamen und eine zweite IP-Aliasadresse hinzu. Verwenden Sie diesen Eintrag für den sicheren Web-Server, der SSL-Anforderungen mit Client-Authentifizierung am Anschluss 443 empfängt.

Bitte beachten Sie, dass diese Host-Aliasnamen und IP-Aliasadressen eindeutig und derselben physischen Maschine zugeordnet sein müssen.

Informationen zur Konfiguration virtueller Host-Namen und IP-Aliasnamen finden Sie in der Dokumentation zum verwendeten DNS-Produkt. Weitere Informationen erhalten Sie in der Dokumentation für den IBM HTTP Server. Sie können beispielsweise auf die Informationen zur Benutzerunterstützung zugreifen, die über die folgende IBM Website für IBM HTTP Server zur Verfügung steht:

`http://www.ibm.com/software/webservers/httpservers/library.html`

Mit dem Directory arbeiten

Das Datenträgerpaket von Tivoli Public Key Infrastructure enthält die für die Installation des IBM Directory erforderliche Software. Sie können die mit Tivoli PKI zur Verfügung gestellte Software installieren und speziell für die Verwendung mit Tivoli PKI konfigurieren oder Tivoli PKI mit einem bereits vorhandenen IBM Directory verwenden. Bei der Installation der Tivoli PKI-Server-Software aktualisieren die Installationsprogramme das Directory mit Informationen, die für die Tivoli PKI-Komponenten erforderlich sind.

Währen der Konfiguration werden von Tivoli PKI Einträge erstellt, die das Programm für Bindevorgänge im Directory und für das Publizieren von Informationen benötigt. So erstellt das Konfigurationsprogramm beispielsweise einen Eintrag für den Tivoli PKI-CA und ordnet ihm die entsprechenden Directory-Zugriffsberechtigungen zu.

Wenn Sie alle Serverkomponenten auf derselben Maschine installieren, aktualisieren die Konfigurationsprogramme das Directory im Hintergrund. Wenn Sie das Directory auf einer fernen Maschine installieren, müssen Sie während der Konfiguration bestimmte Schritte ausführen, um sicherzustellen, dass es korrekt konfiguriert wird. Das Handbuch *Tivoli PKI Konfiguration* enthält Erläuterungen zu dieser Prozedur.

Directory-Schema

Jeder Eintrag im Directory stellt ein einzelnes Objekt dar, wie beispielsweise eine Person, Firma oder Einheit, das durch einen eindeutigen registrierten Namen (Distinguished Name, DN) identifiziert wird. Das Directory-Schema definiert die Regeln für registrierte Namen, wie beispielsweise deren Deklaration sowie die Art der Informationen, die sie enthalten können oder müssen.

Der registrierte Name enthält eine Gruppe von Attributen, durch die das Objekt eindeutig identifiziert werden kann und mit denen die dem Objekt zugeordneten Berechtigungen definiert werden können. Attribute können z. B. die Position eines Objekts, das Unternehmen, dem das Objekt zugeordnet ist, oder den Namen des Objekts angeben.

Um Sie bei der Definition der für Tivoli PKI erforderlichen Directory-Einträge zu unterstützen, stellt das Konfigurations-Applet eine grafische Benutzerschnittstelle (GUI) bereit. Der DN-Editor ermöglicht es Ihnen, DN-Attribute anzugeben, ohne die Anforderungen des Directory-Schemas im Einzelnen zu berücksichtigen.

Directory-Zugriffssteuerung

Alle Directory-Einträge sind logisch in eine hierarchische Struktur integriert. Diese Struktur wird als Directory-Informationsbaumstruktur (Directory Information Tree, DIT) bezeichnet. Diese Verzeichnisbaumstruktur verfügt über eine Root-Ebene und eine beliebige Anzahl von weiteren, untergeordneten Knoten. Jeder Knoten entspricht einem Directory-Eintrag, der durch ein DN-Attribut identifiziert wird.

Das Directory ermöglicht die Definition von Zugriffssteuerungsberechtigungen für einzelne Einträge oder für Einträge und ihre gesamten Unterverzeichnisstrukturen. Bei der Konfiguration von Tivoli PKI werden automatisch die entsprechenden Berechtigungen für die einzelnen DN-Einträge von Tivoli PKI angewendet. Hierbei gilt folgendes:

- Der CA muss auf alle Einträge zugreifen können, die sich in der Directory-Hierarchie auf seinem DN-Eingangspunkt oder darunter befinden. Bei Objekten auf der CA-Basisebene bzw. unterhalb der CA-Basisebene handelt es sich um Objekte, die der Verwaltungsdomäne des CA zugeordnet sind. Diese stellen die Entitäten dar, die berechtigt sind, öffentliche Schlüssel und Zertifikate zu erhalten, die vom CA zertifiziert wurden.
- Da der Tivoli PKI-CA keine direkten Bindevorgänge für das Directory ausführt, verwendet er einen Agenten, der als Directory-Administrator bezeichnet wird. Der Directory-Administrator führt Anforderungen zwischen dem CA, der RA und dem Directory aus. Er ist berechtigt, alle Einträge in der Unterverzeichnisbaumstruktur des CA im Directory zu aktualisieren. Zu dieser Berechtigung gehört die Fähigkeit, Directory-Einträge hinzuzufügen, zu löschen, zu ändern, zu lesen, zu suchen und zu vergleichen.

- Jedes Tivoli PKI-System definiert einen Directory-Root-DN. Der Root-DN ist eine konfigurierte Entität, die in der Directory-Verzeichnisbaumstruktur nicht tatsächlich vorhanden ist. Als Root-Administrator ist der Root-DN berechtigt, alle Knoten im Directory zu aktualisieren, nicht nur die Knoten in der Unterverzeichnisbaumstruktur eines bestimmten CA.

  Die Attribute im Root-DN beschreiben die Protokolle und Steuerelemente, die vom Directory unterstützt werden. Dadurch können Clients wie beispielsweise Tivoli PKI grundlegende Informationen zum Server und zur Directory-Verzeichnisbaumstruktur abrufen. Darüber hinaus ermöglicht es Tivoli PKI, Bindevorgänge für das Directory auszuführen, um Änderungen vorzunehmen.

Mit dem IBM 4758 PCI Cryptographic Coprocessor arbeiten

Dieses Produkt ist zwar optional, es wird jedoch empfohlen, den IBM 4758 PCI Cryptographic Coprocessor zu verwenden, um die optimale Sicherheit für CA- und RA-Unterschriftsschlüssel zu gewährleisten. Schäden auf Grund von Missbrauch durch Systemadministratoren oder unbefugtes Eindringen in das System können so auf ein Minimum reduziert werden.

Anmerkung: Die Unterstützung für den IBM 4758 PCI Cryptographic Coprocessor steht nur in der AIX-Version von Tivoli PKI zur Verfügung.

Der IBM 4758 PCI Cryptographic Coprocessor verwendet die Anwendungsprogrammierschnittstelle (API) der Common Cryptographic Architecture (CCA) von IBM, um leistungsfähige Verschlüsselungsservices zur Verfügung zu stellen. Die gesamte Verschlüsselungsverarbeitung findet innerhalb der sicheren Begrenzung der physischen Verschlüsselungskarte statt.

Während der Installation generiert das IBM 4758-Konfigurationsprogramm einen Hauptschlüssel und speichert diesen in der Hardware. In einem Tivoli PKI-System kann der Koprozessor diesen Hauptschlüssel und einen RSA-Algorithmus verwenden, um den CA- oder RA-Unterschriftsschlüssel dreifach zu verschlüsseln. Dieser Schritt bietet eine weitere Sicherheitsebene gegen Versuche, die CA- oder RA-Unterschrift zu manipulieren oder zu entschlüsseln.

Zusätzlich zur Verschlüsselungsfunktion bietet der IBM 4758 PCI Cryptographic Coprocessor die Möglichkeit, unberechtigten Zugriff auf die Hardware oder den Hauptschlüssel, Unregelmäßigkeiten bei der Spannung und Temperatur sowie zu hohe Strahlung festzustellen. Wird eine solche Unregelmäßigkeit festgestellt, werden die Schlüssel, die für den Zugriff auf die im Modul gesicherten Daten erforderlich sind, zerstört.

Anmerkung: Informationen zum Installieren, Konfigurieren und Klonen des IBM 4758 PCI Cryptographic Coprocessor finden Sie in der Produktdokumentation zur Einheit IBM 4758.

CA- oder RA-Schlüssel in der Hardware speichern

Wenn Sie den IBM 4758 PCI Cryptographic Coprocessor verwenden möchten, müssen Sie ihn auf der Maschine installieren, auf der auch der Tivoli PKI-CA-Server oder Tivoli PKI-RA-Server installiert ist, bevor Sie das Tivoli PKI-System konfigurieren. Bei der Konfiguration des CA bzw. der RA können Sie angeben, ob der Koprozessor zum Speichern des Unterschriftsschlüssels verwendet werden soll.

Bei den meisten Tivoli PKI-Systemen wird der CA- bzw. RA-Schlüssel physisch nicht zusammen mit dem Hauptschlüssel gespeichert. Eine Konfigurationsoption ermöglicht Ihnen jedoch, diesen Standardwert zu überschreiben. Dies wird von IBM aber nicht empfohlen. Wenn in der Hardware des IBM 4758 PCI Cryptographic Coprocessor ein Fehler auftritt, müssen sofort die geeigneten Maßnahmen zur Behebung dieses Fehlers durchgeführt werden.

Wenn Sie den CA- bzw. RA-Schlüssel fest in der Hardware speichern wollen, sollten Sie einen Fehlerbehebungsplan ausarbeiten. Die folgenden Risiken und die entsprechenden Fehlerbehebungsmaßnahmen sind beim festen Speichern des Schlüssels in der Hardware zu beachten:

- Wenn der IBM 4758 PCI Cryptographic Coprocessor gesichert wird, wird lediglich für den Hauptschlüssel, jedoch nicht für die anderen, auf der Hardwarekarte gespeicherten Schlüssel, eine Sicherungskopie erstellt. Wenn die Karte beschädigt wird oder ein anderer Hardwarefehler auftritt, geht der CA- bzw. RA-Unterschriftsschlüssel verloren.
- Wenn der CA- oder RA-Schlüssel verloren geht oder beschädigt wird, müssen Sie den CA bzw. die RA schließen und mit einem neuen Schlüssel erneut starten. Während der CA oder die RA nicht verfügbar sind, können Benutzer, deren Zertifikate vom CA bzw. von der RA unterzeichnet wurden, diese nicht verwenden, da sie nicht geprüft werden können.
- Da die Zertifikate, die mit dem ursprünglichen Schlüssel des CA oder der RA unterzeichnet wurden, nicht mehr gültig sind, müssen nach dem erneuten Einrichten des CA oder der RA neue Zertifikate ausgestellt werden, die mit dem neuen CA- bzw. RA-Schlüssel unterzeichnet sind.

Weitere Informationen zum IBM 4758 PCI Cryptographic Coprocessor finden Sie im Handbuch *Tivoli PKI Systemverwaltung*.

Integration mit dem Policy Director

Der Tivoli Policy Director bietet umfassende Endpunkt-zu-Endpunkt-Sicherheitsfunktionen für Ressourcen, die in Intranets und Extranets über größere Entfernungen hinweg verteilt sind. Er enthält umfassende Unterstützung für die Authentifizierung, Berechtigung, Datensicherheit und Ressourcenverwaltung. Durch die Integration des Policy Director in Tivoli PKI können Sie eine sichere, durch Zertifikate geschützte Umgebung für Ihre e-business-Aktivitäten erstellen.

Der Policy Director stellt einen einzelnen Steuerungspunkt für Web-Umgebungen zur Verfügung. Wenn ein Benutzer versucht, auf eine sichere Site zuzugreifen, kann der Policy Director eine separate Anmeldung für jeden Web-Benutzer anfordern, die Identität des Benutzers authentifizieren und die Berechtigung des Benutzers für den Zugriff auf einen geschützten Bereich überprüfen. Der Policy Director kann so konfiguriert werden, dass er als Teil dieses Prüfungsvorgangs Tivoli PKI-Zertifikate auswertet. So können Sie den Policy Director beispielsweise so konfigurieren, dass er lediglich die Zertifikate akzeptiert, die von einem zuverlässigen CA unterzeichnet wurden, d. h. von einem CA, der dem Policy Director bekannt ist. Indem Sie dem Policy Director ein Tivoli PKI-CA-Zertifikat zur Verfügung stellen, können Sie problemlos eine Sperre zwischen nicht berechtigten Benutzern und den Ressourcen einrichten, die geschützt werden müssen.

Informationen zur Verwendung der Tivoli PKI-Zertifikate in einer Policy Director-Umgebung finden Sie im IBM Redbook *Tivoli SecureWay Policy Director Centrally Managing e-business Security*, IBM Form SG24-6008–00.

Tivoli PKI kann durch den Einsatz von BPOs (Unternehmensprozessobjekten) so angepasst werden, dass eine weitere Integration mit dem Policy Director erzielt werden kann. Es ist z. B. möglich, ein BPO zu schreiben, mit dem nach der Genehmigung einer Zertifikatsanforderung eine Policy Director-Benutzer-ID erstellt werden kann. Auf diese Weise wird eine Bindung zwischen dem Zertifikat und dem ePerson-Objekt von Policy Director erstellt, das in LDAP generiert wurde. Die Bereitstellung eines BPOs mit dieser Funktionalität hat den zusätzlichen Vorteil, dass ein webbasierter Registrierungsmechanismus für Policy Director zur Verfügung gestellt wird.

Informationen zum Entwickeln und Anpassen von Unternehmensprozessobjekten (BPOs) an Ihre individuellen Unternehmensanforderungen finden Sie im IBM Redbook *Working with Business Process Objects for Tivoli SecureWay PKI*, IBM Form SG24-6043-00.

Unterstützte Serverkonfigurationen

Sie könne alle Tivoli PKI-Server-Komponenten auf einer einzigen Maschine installieren oder die Verarbeitung auf mehrere Maschinen verteilen. Hierbei müssen allerdings die folgenden Einschränkungen berücksichtigt werden:

- Der Webserver, WebSphere und der Hauptserver von Tivoli PKI, der den RA-Server sowie die Datenbanken mit den Konfigurations- und Registrierungsdaten umfasst, müssen auf der selben Maschine ausgeführt werden.
- Der CA- und der Prüfserver sowie die zugehörigen Datenbanken müssen ebenfalls auf einer Maschine installiert werden.
- Der Directory-Server und die zugehörige Datenbank müssen sich auf der selben Maschine befinden.

Die Konfiguration des Servernetzes ist abhängig vom erwarteten Arbeitsaufkommen in Ihrem Unternehmen sowie von der Verwendung einer bestimmten Maschine für verschiedene Zwecke. Wenn Sie beispielsweise das Directory bereits installiert haben und mit anderen Anwendungen verwenden, empfiehlt es sich möglicherweise, diesen Server nicht für die anderen Tivoli PKI-Komponenten zu konfigurieren.

Nachfolgend sind die Konfigurationsmöglichkeiten für die Verteilung der Serverkomponenten zusammengefasst:

- Der Haupt-Server von Tivoli PKI, der CA- und Prüf-Server und der Directory-Server auf einer Maschine.
- Der Haupt-Server von Tivoli PKI, der CA- und Prüf-Server und der Directory-Server auf drei separaten Maschinen.
- Der Haupt-Server von Tivoli PKI auf einer Maschine; der CA- und Prüf-Server und der Directory-Server auf einer zweiten Maschine.

- Der Haupt-Server von Tivoli PKI und der CA- und Prüf-Server auf einer Maschine; der Directory-Server auf einer zweiten Maschine.
- Der Haupt-Server von Tivoli PKI und der Directory-Server auf einer Maschine; der CA- und Prüf-Server auf einer zweiten Maschine.

Hinweise zu länderübergreifenden Umgebungen

Die Tivoli PKI-Komponenten unterstützen den Einsatz in einer länderübergreifenden Umgebung:

- Nachrichtendateien und grafische Benutzerschnittstellen (GUIs) wurden übersetzt und stellen Unterstützung in den folgenden Landessprachen zur Verfügung: Englisch, Französisch, Deutsch, Italienisch, Spanisch, brasilianisches Portugiesisch, Japanisch, Koreanisch, vereinfachtes Chinesisch und traditionelles Chinesisch.
- Alle Texteingabefelder unterstützen Unicode über die UTF-8-Verschlüsselung.
- Alle registrierten Namen (DN) unterstützen Unicode über die UTF-8-Verschlüsselung.

Unter Tivoli PKI stehen alle Verzeichnispfade in den Konfigurationsdateien ausschließlich in Englisch zur Verfügung und müssen im ASCII-Format angegeben werden.

Aufgrund von Exportbestimmungen der US-Regierung wird das Tivoli PKI-Produkt in verschiedenen Verschlüsselungsstufen (Encryption Editions) ausgeliefert. Die für US-Kunden (USA, US-Niederlassungen und Kanada) verfügbare Verschlüsselungsstufe enthält einen stärkeren Verschlüsselungsalgorithmus als die international verfügbare Ausgabe. Die Verschlüsselungsalgorithmen sind im Produktcode vorab festgelegt und können bei der Installation, Konfiguration oder Verwendung des Produkts nicht geändert werden.

Tivoli PKI-Datenträgerpaket

Die Software für Tivoli PKI wird in einem Datenträgerpaket ausgeliefert, das die folgenden CDs enthält:

- *CD für IBM WebSphere Application Server for AIX Standard Edition V3.5 Application Server und IBM HTTP Server*

  Diese CD enthält die Webserversoftware, die für Tivoli PKI erforderlich ist. Darüber hinaus enthält sie WebSphere Application Server und IBM HTTP Server.

- *CD für IBM WebSphere Application Server for AIX Standard Edition V3.5 IBM Directory*

  Diese CD enthält die für Tivoli PKI erforderliche Datenbank- und Directory-Software.

- *CD 1 für Tivoli Public Key Infrastructure für AIX V 3.7.1*

  Diese CD enthält die für Tivoli PKI erforderliche Datenbanksoftware und folgende Komponenten:

  - Die Tivoli PKI-RA, den Zertifikatsaussteller und den Prüf-Server, die Directory-Software sowie Programme für die Installation, Konfiguration und Verwaltung des Produkts.
  - Installations-Image für das Applet Tivoli PKI RA Desktop.

  Plattformspezifische CDs stehen für das Betriebssystem AIX zur Verfügung.

- *CD 2 für Tivoli Public Key Infrastructure für AIX V 3.7.1*

  Diese CD enthält die für Tivoli PKI erforderliche Software und verschiedene Programmkorrekturen.

- *Tivoli Public Key Infrastructure Einführung*
- *Release-Informationen für Tivoli Public Key Infrastructure*

4

Tivoli PKI unter AIX installieren

Das vorliegende Kapitel enthält Prozeduren zum Installieren von Tivoli Public Key Infrastructure (PKI) sowie der für den Betrieb erforderlichen Produkte auf einer AIX-Plattform.

Vor dem Installieren der Tivoli PKI-Software sollten Sie unbedingt die neueste Version der Release-Informationen für das Produkt lesen. Die aktuellste Version der Release-Informationen können Sie über die Website von Tivoli Public Key Infrastructure abrufen:

`http://www.tivoli.com/support`

Installieren Sie die Software für Tivoli PKI in der folgenden Reihenfolge:

1. Betriebssystem AIX Version 4.3.3.
2. Wartungsstufe 6 des Betriebssystems AIX (mit anschließendem Warmstart der Maschine).
3. IBM DB2 Universal Database Version 6.1 Fix Pack 4.
4. IBM Directory Server Version 3.1.1.5
5. IBM Developer Kit für AIX, Java Technology Edition, Version 1.2.2 PTF 8
6. IBM WebSphere Application Server Standard Edition Version 3.5
7. Führen Sie ein Upgrade für IBM WebSphere Application Server Standard Edition Version 3.5 PTF 4 durch.

8. Inaktivieren Sie die Funktion für den automatischen Start von IBM HTTP Server.
9. Starten Sie WebSphere Application Server.
10. IBM KeyWorks Version 1.1.3.1.
11. Tivoli PKI-Serversoftware.

AIX konfigurieren

Gehen Sie anhand der folgenden Richtlinien vor, wenn Sie die AIX-Software auf der Maschine bzw. den Maschinen installieren, auf der/denen die Tivoli PKI-Software installiert werden soll. Wenn Sie AIX bereits installiert haben, können Sie diese Richtlinien als Prüfliste verwenden, um sicherzustellen, dass alle Dateien installiert wurden, die für die Tivoli PKI-Komponenten erforderlich sind.

Wenn Sie Tivoli PKI in einer Konfiguration mit mehreren Maschinen installieren wollen, müssen Sie auf allen Maschinen, auf denen eine Server-Komponente von Tivoli PKI installiert werden soll, zuerst AIX installieren.

Gehen Sie wie folgt vor, um den Installationsprozess zu starten:

1. Führen Sie eine Neuinstallation (**Neu installieren und überschreiben**), keine Erhaltungsinstallation (**Installation mit Erhalten**) durch.

   Anmerkung: Installieren Sie zu diesem Zeitpunkt keine Fix-Versionen. Dieser Arbeitsschritt wird in einer späteren Phase des Installationsprozesses ausgeführt.

2. Stellen Sie sicher, dass für die länderspezifischen Angaben der Maschine die Sprache definiert ist, in der Sie die Tivoli PKI-Anwendungen ausführen möchten.
3. Tivoli PKI unterstützt AIX TCB (Trusted Computing Base = gesicherte Computerbasis). Wenn Sie diese Funktion verwenden möchten, die die Sicherheit des verwendeten Betriebssystems weiter erhöht, wählen Sie diese Option aus, um sie bei der Installation von AIX zu aktivieren.

4. Bei der TCP/IP-Konfiguration müssen Sie den Kurznamen des Systems als Hostnamen angeben. Geben Sie z. B. **hostname** an Stelle von “hostname.mycompany.com” ein. Gehen Sie nach der AIX-Installation wie folgt vor, um die korrekte Angabe des Namens zu prüfen:

   a. Geben Sie **smitty** ein.

   b. Wählen Sie die Option für **Netzkommunikation und -Anwendungen** aus.

   c. Wählen Sie die Option für **TCP/IP** aus.

   d. Wählen Sie die Option **Mindestkonfiguration & Systemstart** aus.

   e. Wählen Sie in der Liste der verfügbaren Netzschnittstellen den gewünschten Eintrag aus. Verwenden Sie z. B. **en0 Standard Ethernet Network Interface**.

   f. Prüfen Sie, ob der für HOSTNAME angegebene Wert das korrekte Format aufweist.

Dateien prüfen

Nach der Installation von AIX und dem Neustart des Systems müssen Sie prüfen, ob die folgenden Dateien erfolgreich installiert wurden:

```
bos.adt.base              4.3.3.0  COMMITTED  Base Application Development
bos.adt.debug             4.3.3.0  COMMITTED  Base Application Development
bos.adt.graphics          4.3.3.0  COMMITTED  Base Application Development
bos.adt.include           4.3.3.0  COMMITTED  Base Application Development
bos.adt.lib               4.3.3.0  COMMITTED  Base Application Development
bos.adt.libm              4.3.3.0  COMMITTED  Base Application Development
bos.adt.prof              4.3.3.0  COMMITTED  Base Profiling Support
bos.adt.prt_tools         4.3.3.0  COMMITTED  Printer Support Development
bos.adt.samples           4.3.3.0  COMMITTED  Base Operating System Samples
bos.adt.sccs              4.3.3.0  COMMITTED  SCCS Application Development
bos.adt.syscalls          4.3.3.0  COMMITTED  System Calls Application
bos.adt.utils             4.3.3.0  COMMITTED  Base Application Development
bos.adt.data              4.3.0.0  COMMITTED  Base Application Development
X11.adt.bitmaps           4.3.0.0  COMMITTED  AIXwindows Application
X11.adt.ext               4.3.3.0  COMMITTED  AIXwindows Application
X11.adt.imake             4.3.3.0  COMMITTED  AIXwindows Application
X11.adt.include           4.3.3.0  COMMITTED  AIXwindows Application
X11.adt.lib               4.3.3.0  COMMITTED  AIXwindows Application
X11.adt.motif             4.3.3.0  COMMITTED  AIXwindows Application
X11.apps.aixterm          4.3.3.0  COMMITTED  AIXwindows aixterm Application
X11.apps.clients          4.3.3.0  COMMITTED  AIXwindows Client Applications
X11.apps.config           4.3.3.0  COMMITTED  AIXwindows Configuration
X11.apps.custom           4.3.3.0  COMMITTED  AIXwindows Customizing Tool
X11.apps.msmit            4.3.3.0  COMMITTED  AIXwindows msmit Application
X11.apps.rte              4.3.3.0  COMMITTED  AIXwindows Runtime
```

```
X11.apps.util              4.3.3.0  COMMITTED  AIXwindows Utility
X11.apps.xterm             4.3.3.0  COMMITTED  AIXwindows xterm Application
X11.base.common            4.3.3.0  COMMITTED  AIXwindows Runtime Common
X11.base.lib               4.3.3.0  COMMITTED  AIXwindows Runtime Libraries
X11.base.rte               4.3.3.0  COMMITTED  AIXwindows Runtime Environment
X11.base.smt               4.3.3.0  COMMITTED  AIXwindows Runtime Shared
X11.compat.lib.X11R5       4.3.3.0  COMMITTED  AIXwindows X11R5 Compatibility
X11.fnt.coreX              4.3.0.0  COMMITTED  AIXwindows X Consortium Fonts
X11.fnt.defaultFonts       4.3.2.0  COMMITTED  AIXwindows Default Fonts
X11.fnt.iso1               4.3.3.0  COMMITTED  AIXwindows Latin 1 Fonts
X11.motif.lib              4.3.3.0  COMMITTED  AIXwindows Motif Libraries
X11.motif.mwm              4.3.3.0  COMMITTED  AIXwindows Motif Window
ifor_ls.base.cli           4.3.3.0  COMMITTED  License Use Management Runtime
ifor_ls.client.base        4.3.3.0  COMMITTED  License Use Management Client
ifor_ls.client.gui         4.3.3.0  COMMITTED  License Use Management Client
ifor_ls.msg.en_US.base.cli
ifor_ls.base.cli           4.3.3.0  COMMITTED  License Use Management Runtime
ifor_ls.client.base        4.3.3.0  COMMITTED  License Use Management Client
xlC.cpp                    4.3.0.1  COMMITTED  C for AIX Preprocessor
Java.rte.bin               1.1.8.0  COMMITTED  Java Runtime Environment
Java.rte.classes           1.1.8.0  COMMITTED  Java Runtime Environment
Java.rte.lib               1.1.8.0  COMMITTED  Java Runtime Environment
```

Wenn nicht alle diese Dateien installiert sind, müssen Sie die fehlenden Dateien nachinstallieren, bevor Sie die Installation fortsetzen.

Ausreichende Paging-Bereiche prüfen

Als Paging-Bereich müssen mindestens 768 MB zur Verfügung stehen. Führen Sie die folgenden Arbeitsschritte aus, um zu prüfen, ob ein ausreichender Paging-Bereich vorhanden ist:

1. Geben Sie **smitty** ein.
2. Wählen Sie die Option für **Systemspeicherverwaltung (physischer und logischer Speicher)** aus.
3. Wählen Sie die Option für den **Logical Volume Manager** aus.
4. Wählen Sie die Option für den **Paging-Bereich** aus.
5. Wählen Sie die Option für **Paging-Bereiche auflisten** aus.
6. Gehen Sie wie folgt vor, wenn als Gesamtgröße nicht mindestens 768 MB angegeben wird:
   a. Drücken Sie die Taste **F3** oder **Abbrechen**.
   b. Wählen Sie die Option für **Merkmale eines Paging-Bereichs ändern / anzeigen** aus.
   c. Wählen Sie den Namen des Paging-Bereichs aus, dessen Größe erhöht werden soll.

d. Fügen Sie die Anzahl der zusätzlichen logischen Partitionen hinzu, die erforderlich sind, um den Paging-Bereich auf 768 MB zu vergrößern.

Fix-Version auf AIX anwenden

Nach der Prüfung der Dateien für AIX müssen Sie die Fix-Version ML 4330–06 installieren. Fordern Sie die Programmkorrektur AIX Fix-Version ML 4330–06 an, und installieren Sie diese entsprechend der zugehörigen Dokumentation. Nach der Anwendung dieser Fix-Version müssen Sie die Maschine erneut starten.

AIX-Datenträgergruppen und -Dateisysteme konfigurieren

Verwenden Sie das AIX System Management Interface Tool (SMIT), um die folgenden Dateisysteme zu konfigurieren. Dieser Konfigurationsvorschlag basiert auf der Verwendung von zwei Plattenlaufwerken mit 4,5 GB freiem Speicherplatz für die Datenträgergruppen rootvg und datavg.

Anmerkung: Bei diesen Konfigurationsvorschlägen wird davon ausgegangen, dass alle Server-Komponenten auf derselben Maschine installiert werden. Wenn Sie den Zertifikatsaussteller und das Prüfsubsystem auf einer Maschine installieren, bei der es sich nicht um den RA-Server handelt, müssen Sie die Prozedur entsprechend anpassen.

- Für die rootvg-Partition:
  - Definieren Sie für die Root-Partition (/) 64 MB (128.000 512-Byte-Blöcke).
  - Definieren Sie für die /usr-Partition 3 GB (6.000.000 512-Byte-Blöcke).
  - Definieren Sie für die /tmp-Partition 200 MB (400.000 512-Byte-Blöcke).
  - Definieren Sie für die /var-Partition 500 MB (1.000.000 512-Byte-Blöcke).

- Definieren Sie für die /home-Partition 200 MB (400.000 512-Byte-Blöcke).

- Für die datavg-Partition:
  - Definieren Sie für die /local-Partition 2 GB (4.000.000 512-Byte-Blöcke).
  - Erstellen Sie eine /dbfsibm-Partition, und definieren Sie für diese 500 MB (1.000.000 512-Byte-Blöcke).

    Dies ist das Standarddateisystem für den Tivoli PKI-CA. Möglicherweise muss die Größe angepasst werden, um der Anzahl der ausgestellten Zertifikate zu entsprechen.
  - Erstellen Sie eine /dbfspkrf-Partition, und definieren Sie für diese 300 MB (600.000 512-Byte-Blöcke).

    Dies ist das Standarddateisystem für die Registrierungsfunktion. Beachten Sie hierbei, dass die Größe möglicherweise entsprechend der Anzahl der Benutzer angepasst werden muss, die eine Zertifikatsregistrierung durchführen.
  - Erstellen Sie eine /dbfsadt-Partition, und definieren Sie für diese 300 MB (600.000 512-Byte-Blöcke).

    Dies ist das Standarddateisystem für das Prüfsubsystem. Beachten Sie hierbei, dass die Größe möglicherweise entsprechend der Anzahl der Prüfereignisse angepasst werden muss, die protokolliert werden sollen.
  - Erstellen Sie eine /dbfskrb-Partition, und definieren Sie für diese 300 MB (600.000 512-Byte-Blöcke).

    Dies ist das Standarddateisystem für die Funktion zur Schlüsselsicherung und -wiederherstellung. Beachten Sie hierbei, dass die Größe möglicherweise entsprechend der Anzahl der ausgegebenen Anforderungen für die Schlüsselsicherung angepasst werden muss.

CD-ROM-Dateisystem erstellen

Wenn Sie Tivoli PKI sowie die hierfür erforderlichen Produkte installieren wollen, müssen Sie ein CD-ROM-Dateisystem als '/cdrom' anhängen. Bei Bedarf können Sie mit dem folgenden Befehl eine Definition für dieses Dateisystem erstellen:

```
crfs -v cdrfs -d /dev/cd0 -m /cdrom -p ro -A no
```

Alternativ hierzu können Sie für die Erstellung des Dateisystems auch SMIT verwenden:

```
smitty crcdrfs
```

Anzahl der AIX-Systembenutzer ändern

Geben Sie den folgenden Befehl ein, um die Anzahl der AIX-Systembenutzer zu ändern. Sie müssen anschließend einen Neustart für das System durchführen, damit dieser Befehl wirksam wird.

```
chlicense -u 100
```

Hostnamensauflösung sicherstellen

Gehen Sie wie folgt vor, um AIX so zu konfigurieren, dass Ihr lokaler Server Hostnamen korrekt auflösen kann:

1. Erstellen Sie im Verzeichnis '/etc' eine Datei mit dem Namen 'netsvc.conf', die nur die folgende Zeile enthält, und beachten Sie hierbei, dass in dieser Anweisung keine Leerzeichen enthalten sind:

   ```
   hosts=local,bind4
   ```

   Sie können diese Datei mit einem Texteditor wie z. B. 'vi' oder durch Eingabe des folgenden Befehls erstellen:

   ```
   echo hosts=local,bind4 > netsvc.conf
   ```

2. Editieren Sie die Datei '/etc/hosts', und prüfen Sie hierbei, ob in der Datei auf den Server verwiesen wird, den Sie momentan konfigurieren. Beispiel:

   ```
   127.0.0.1       loopback                localhost
   192.40.168.20   taserver.company.com    taserver
   ```

   Die zweite Zeile im vorherigen Beispiel enthält die IP-Adresse, den vollständig qualifizierten Hostnamen sowie den Hostkurznamen des AIX-Servers, den Sie momentan konfigurieren.

3. Erstellen Sie die Datei '/etc/resolv.conf', oder ändern Sie diese so, dass sie lediglich die folgenden Zeilen enthält:

```
domain      company.com
nameserver  10.10.10.90
```

   Die erste Zeile im vorherigen Beispiel enthält den Domänennamen des Servers, den Sie momentan konfigurieren. Die zweite Zeile enthält die IP-Adresse des DNS-Namens-Servers.

Systemimage erstellen

Obwohl dies nicht zwingend erforderlich ist, empfiehlt IBM, die AIX-Systemkonfiguration zu sichern, bevor die Installation von Tivoli PKI fortgesetzt wird. Mit Hilfe eines Sicherungs-Images kann das System wiederhergestellt werden, falls Probleme auftreten.

Geben Sie folgende Befehle als Root ein und wählen Sie die gewünschten Optionen aus, um ein System-Image zu erstellen:

```
smitty mksysb
smitty savevg
```

Datenbanksoftware installieren

Tivoli PKI verwendet zum Verwalten von Daten IBM DB2 Universal Database. Die Software von IBM DB2 Universal Database wird zusammen mit IBM WebSphere Application Server Standard Edition Version 3.5.0 bereitgestellt. Die Software von IBM DB2 Universal Database, die zusammen mit IBM WebSphere Application Server bereitgestellt wird, dient nur zur Verwendung durch Tivoli PKI-Anwendungen. Wenn Sie die Datenbanksoftware anpassen oder zusammen mit anderen Anwendungen als Tivoli PKI verwenden wollen, müssen Sie eine Lizenz für eine Vollversion von IBM DB2 Enterprise Edition, Version 6.1 kaufen.

Die folgenden Abschnitte enthalten eine Beschreibung der Prozeduren für die Installation der Datenbanksoftware. Wenn Sie Tivoli PKI in einer Konfiguration mit mehreren Maschinen installieren wollen, müssen Sie auf allen Maschinen, auf denen eine Serverkomponente von Tivoli PKI installiert werden soll, zuerst die Datenbanksoftware installieren. Beachten Sie hierbei die folgenden Richtlinien:

- Während der Konfiguration erstellt Tivoli PKI automatisch die Datenbanken, die für die Server-Programme erforderlich sind. Auch die Directory-Datenbank wird von Tivoli PKI erstellt, falls sie nicht bereits vorhanden ist.
- Vor der Installation von Tivoli PKI muss sichergestellt werden, dass die erforderliche Version der Datenbanksoftware auf allen Maschinen installiert ist, auf denen eine Tivoli PKI-Server-Komponente installiert werden soll. Stellen Sie darüber hinaus sicher, dass das Datenbanksystem eigenständig korrekt ausgeführt wird, bevor Sie Tivoli PKI installieren.

DB2 installieren

Führen Sie die nachfolgend beschriebene Prozedur aus, um die Datenbank-Basissoftware zu installieren.

1. Melden Sie sich als Benutzer mit Root-Berechtigung an.
2. Legen Sie die CD von *IBM WebSphere Application Server für AIX* in das CD-ROM-Laufwerk ein. Geben Sie den folgenden Befehl ein, um die CD anzuhängen:

   ```
   mount /cdrom
   ```
3. Geben Sie den folgenden Befehl ein, um in das Verzeichnis /Db2 auf der CD zu wechseln:

   ```
   cd /cdrom/Db2
   ```
4. Geben Sie folgenden Befehl ein, um das Script für die Datenbankinstallation auszuführen:

   ```
   ./db2setup
   ```

   Während der Installation prüft das Datenbankinstallations-Script, ob bereits eine vorherige Version von DB2 auf dem System installiert ist und ob auf der gewünschten Maschine genügend Plattenspeicherplatz zur Verfügung steht. Steht auf der Maschine nicht ausreichend Speicherplatz zur Verfügung, wird der freie Speicherplatz für das Dateisystem ’/usr’ auf 400 MB erhöht.
5. Wählen Sie **DB2 UDB Enterprise Edition** aus.
6. Wählen Sie **DB2-Produktnachrichten** aus.

7. Wählen Sie die gewünschte Sprache aus, und klicken Sie anschließend auf **OK**.
8. Wählen Sie **DB2-Produktbibliothek** aus.
9. Wählen Sie die gewünschte Sprache aus, und klicken Sie anschließend auf **OK**.
10. Wählen Sie **OK** aus.
11. Wählen Sie unter **DB2-Services erstellen** die Option **DB2-Exemplar erstellen** aus.
12. Drücken Sie die **Eingabetaste**.
13. Geben Sie als **Benutzername** die Zeichenfolge **db2inst1** und als **Benutzerverzeichnis** das Verzeichnis **/home/db2inst1** an. Übernehmen Sie für alle anderen Werte die Standardeinstellungen.
14. Geben Sie Werte für das **Kennwort** und das **Prüfkennwort** ein.
15. Wählen Sie **Merkmale** aus.
16. Drücken Sie die **Eingabetaste**.
17. Wählen Sie als **Identifikationsüberprüfungsart** den Wert **Client** aus.
18. Wählen Sie **OK** aus.
19. Wählen Sie **OK** aus.
20. Geben Sie für die **Authentifizierung** Werte für **Kennwort** und **Prüfkennwort** des Benutzernamens db2fenc1 ein.
21. Wählen Sie **OK** aus.
22. Wählen Sie **OK** aus.
23. Wählen Sie **OK** aus.

    Anmerkung: Ignorieren Sie die Warnung.
24. Wählen Sie **Weiter** aus.
25. Wählen Sie **OK** aus.

    Die DB2-Installation wird nun gestartet.

26. Wählen Sie **OK** aus.
27. Wählen Sie **OK** aus, um die Verarbeitung zu beenden oder das Protokoll anzuzeigen.
28. Wählen Sie **Schließen** aus.
29. Wählen Sie **OK** aus.
30. Wählen Sie **OK** aus.

    Diese Phase der Installation ist nun abgeschlossen.
31. Geben Sie den folgenden Befehl ein, um den Tivoli PKI-Datenträger abzuhängen:

    ```
    umount /cdrom
    ```
32. Geben Sie den folgenden Befehl ein, um in das entsprechende Verzeichnis zu wechseln:

    ```
    cd /usr/lpp/db2_06_01/cfg
    ```
33. Geben Sie den folgenden Befehl ein, um die Umgebungsvariablen zu definieren:

    ```
    ./db2ln
    ```
34. Setzen Sie die Installation fort, und lesen Sie hierzu die Informationen im Abschnitt „IBM Directory installieren” auf Seite 67.

IBM Directory installieren

Tivoli PKI verwendet das IBM Directory , um Informationen zu Zertifikaten, die von der Registrierungsfunktion ausgestellt wurden, zu speichern und zu verwalten. Verwenden Sie die in den folgenden Abschnitten beschriebenen Prozeduren, um die Directory-Software zu installieren und zu konfigurieren. Sie können diese Software auf einer fernen Maschine oder auf der Maschine installieren, auf der auch eine Tivoli PKI-Server-Komponente installiert werden soll.

Directory-Software installieren

Führen Sie mit Root-Berechtigung die folgenden Arbeitsschritte aus:

1. Legen Sie die CD für Directory Server Version 3.1.1.5 in das CD-ROM-Laufwerk Ihres Systems ein. Geben Sie den folgenden Befehl ein, um die CD anzuhängen:

   ```
   mount /cdrom
   ```

2. Geben Sie den folgenden Befehl ein, um in das entsprechende Verzeichnis zu wechseln:

   ```
   cd /cdrom/usr/sys/inst.images
   ```

3. Geben Sie den folgenden Befehl ein:
   ```
   smitty install
   ```
4. Wählen Sie **Software installieren und aktualisieren** aus.
5. Wählen Sie **Neueste verfügbare Software installieren und aktualisieren** aus.
6. Wählen Sie für die Option **EINGABE-Einheit/Verzeichnis für Software .** (Punkt) aus.
7. Drücken Sie unter **Neueste verfügbare Software installieren und aktualisieren** die Taste **F4**, um eine Liste der für die Installation verfügbaren Dateien anzuzeigen.
8. Drücken Sie die Taste **F7**, um die Datei 'ldap.client' für die Installation auszuwählen.
9. Drücken Sie nach der Installation dieser Datei unter **Neueste verfügbare Software installieren und aktualisieren** die Taste **F4**, um eine Liste der für die Installation verfügbaren Dateien anzuzeigen.
10. Drücken Sie die Taste **F7**, um die folgenden Dateien für die Installation auszuwählen:
    - ldap.server
    - ldap.html.en_US

    Anmerkung: Sie müssen die korrekten Sprachdateien für Ihre Installation auswählen.
11. Geben Sie die folgenden Befehle ein, um den Directory-Datenträger abzuhängen. Wenn Sie diese Befehle eingeben, kann kein Prozess auf Teile der Verzeichnisbaumstruktur von '/cdrom' zugreifen:
    ```
    umount /cdrom
    ```

Anmerkung: In einer Konfiguration mit mehreren Maschinen müssen Sie auf jedem Tivoli PKI-Server die Directory-Client-Software installieren, bevor Sie das Konfigurations-Applet für Tivoli PKI ausführen. Zum Installieren dieser Software müssen Sie die Option 'ldap.client' von der CD für den Directory Server auf allen

Maschinen außer auf der Einheit installieren, auf der soeben die Directory-Server-Software installiert wurde. Der Name der wichtigen Datei, die auf allen Maschinen installiert werden muss, lautet 'libldap.a'.

Nach Abschluss dieser Arbeitsschritte sind die folgenden Dateien installiert:

```
ldap.client.adt        3.1.1.5 COMMITTED SecureWay Directory Client SDK
ldap.client.rte        3.1.1.5 COMMITTED SecureWay Directory Client
ldap.html.en_US.config 3.1.1.0 COMMITTED SecureWay Directory
ldap.html.en_US.man    3.1.1.0 COMMITTED SecureWay Directory Man Pages
ldap.msg.en_US         3.1.1.0 COMMITTED SecureWay Directory Messages -
ldap.server.admin      3.1.1.5 COMMITTED SecureWay Directory Server
ldap.server.com        3.1.1.5 COMMITTED SecureWay Directory Server
ldap.server.rte        3.1.1.5 COMMITTED SecureWay Directory Server
ldap.client.rte        3.1.1.5 COMMITTED SecureWay Directory Client
ldap.server.admin      3.1.1.5 COMMITTED SecureWay Directory Server
ldap.server.com        3.1.1.5 COMMITTED SecureWay Directory Server
```

Java installieren

Gehen Sie wie folgt vor, um Java zu installieren:

1. Legen Sie die CD von *Tivoli PKI für AIX* in das CD-ROM-Laufwerk Ihres Systems ein. Geben Sie den folgenden Befehl ein, um die CD anzuhängen:

   ```
   mount /cdrom
   ```

2. Geben Sie den folgenden Befehl ein, um in das entsprechende Verzeichnis zu wechseln:

   ```
   cd /cdrom/aix/Java_1.2.2.ptf8
   ```

3. Geben Sie den folgenden Befehl ein:

   ```
   smitty install
   ```

4. Wählen Sie **Software installieren und aktualisieren** aus.
5. Wählen Sie **Neueste verfügbare Software installieren und aktualisieren** aus.
6. Wählen Sie für die Option **EINGABE-Einheit/Verzeichnis für Software .** (Punkt) aus.
7. Drücken Sie die **Eingabetaste**.

8. Drücken Sie die **Eingabetaste**.
9. Drücken Sie die Taste **F10**.
10. Geben Sie die folgenden Befehle ein, um den Tivoli PKI-Datenträger abzuhängen. Wenn Sie diesen Befehl eingeben, kann kein Prozess auf Teile der Verzeichnisbaumstruktur von '/cdrom' zugreifen:

    ```
    umount /cdrom
    ```

Nach Abschluss dieser Arbeitsschritte sind die folgenden Dateien installiert:

```
Java_dev2.adt.debug     1.2.2.9 COMMITTED Java Application Development
Java_dev2.adt.includes  1.2.2.0 COMMITTED Java Application Development
Java_dev2.adt.src       1.2.2.9 COMMITTED Java Classes Source Code
Java_dev2.rte.bin       1.2.2.9 COMMITTED Java Runtime Environment
Java_dev2.rte.lib       1.2.2.9 COMMITTED Java Runtime Environment
```

WebSphere Application Server-Datenbank erstellen

Vor der Installation von WebSphere Application Server müssen Sie die zugehörige DB2-Datenbank erstellen. Gehen Sie hierzu wie folgt vor:

1. Melden Sie sich als Benutzer mit Root-Berechtigung an.
2. Geben Sie den folgenden Befehl ein:

   ```
   su - db2inst1
   ```
3. Starten Sie die DB2-Konsole mit dem folgenden Befehl:

   ```
   db2
   ```
4. Erstellen und konfigurieren Sie die Datenbank für WebSphere Application Server mit den folgenden Befehlen:

   ```
   create database was_db
   update db cfg for was_db using applheapsz 256
   ```
5. Verlassen Sie die DB2-Konsole durch Eingabe von **quit**.
6. Stoppen Sie DB2 durch Eingabe von **db2stop**.
7. Starten Sie DB2 durch Eingabe von **db2start**.
8. Geben Sie den folgenden Befehl ein: **exit**.

Webserversoftware installieren

Tivoli PKI verwendet zur Unterstützung seiner Web-basierten Funktionen IBM WebSphere Application Server und IBM HTTP Server. Befolgen Sie beim Installieren der Software auf einer AIX-Plattform die angegebene Prozedur, um sicherzustellen, dass die Web-Server-Programme für den Einsatz mit Tivoli PKI korrekt installiert sind. Sie müssen die Software auf der Maschine installieren, auf der auch die RA-Komponente installiert werden soll.

Obwohl WebSphere über eine Verwaltungsschnittstelle zum Verwalten von Servlets verfügt, ist es weder möglich noch erforderlich, Tivoli PKI-Servlets mit dieser Schnittstelle zu verwalten.

Nach der Installation von Tivoli PKI aktualisiert ein Installationsabschlussprogramm den Web-Server mit den für Tivoli PKI erforderlichen Informationen. Wenn Sie den Web-Server starten, verwendet dieser die Konfigurationsdatei, die Tivoli PKI zu diesem Zweck erstellt hat.

Anmerkung: Lesen Sie unbedingt die Informationen dazu, wie Tivoli PKI Ports auf dem Web-Server konfiguriert, die in „IP-Aliasnamen für den Webserver konfigurieren” auf Seite 44 enthalten sind. Wenn Sie die Ports auf Ihrem System anders konfigurieren wollen, müssen Sie dies vor der Konfiguration von Tivoli PKI tun.

WebSphere Application Server installieren

1. Melden Sie sich als Benutzer mit Root-Berechtigung an.
2. Legen Sie die CD von *WebSphere Application Server für AIX* in das CD-ROM-Laufwerk ein. Geben Sie den folgenden Befehl ein, um die CD anzuhängen:

   ```
   mount /cdrom
   ```
3. Bei einer fernen Installation müssen Sie WebSphere in einer grafischen X11-Umgebung installieren. Geben Sie den folgenden Befehl ein, um die korrekte Umgebungsvariable ’DISPLAY’ zu

exportieren, die durch das WebSphere-Installationsprogramm geöffnet werden muss. Hierbei steht *yourhost:0.0* für den richtigen Wert für Ihr System:

```
export DISPLAY=yourhost:0.0
```

4. Installieren Sie WebSphere, und gehen Sie hierzu wie folgt vor:

   a. Geben Sie den folgenden Befehl ein, um in das entsprechende Verzeichnis zu wechseln:

      ```
      cd /cdrom/aix
      ```

   b. Geben Sie folgenden Befehl ein, um das Script 'install.sh' auszuführen.

      ```
      ./install.sh
      ```

   c. Klicken Sie im Eingangsfenster auf **Weiter**.

   d. Wählen Sie im Fenster mit den Installationsoptionen die Option für die **Angepasste Installation** aus, und klicken Sie anschließend auf **Weiter**.

   e. Wählen Sie im ersten Fenster zur Auswahl der Anwendungsserverkomponenten die Option für **Alle Komponenten** aus, und klicken Sie anschließend auf **Weiter**.

   f. Wählen Sie im zweiten Fenster zur Auswahl der Anwendungsserverkomponenten die Option für die **IBM HTTP Server-Plug-ins** aus, und klicken Sie dann auf **Weiter**.

   g. Wählen Sie im Fenster mit den Datenbankoptionen in der Drop-down-Liste für den Datenbanktyp die Option für **DB2** aus, und geben Sie in den folgenden Feldern die u. a. Werte an:

      Datenbankname: was_db
      DB-Benutzerverzeichnis: /home/db2inst1
      Benutzer-ID für Datenbank: db2inst1
      Datenbankkennwort: *yourpassword*
      Kennwort bestätigen: *yourpassword*

      Hierbei steht *yourpassword* für das Kennwort von db2inst1, das bei der Ausführung von db2setup eingegeben wurde.

h. Geben Sie im Fenster mit den Sicherheitsinformationen das Root-Kennwort für das System ein, bestätigen Sie dieses, und klicken Sie anschließend auf **Weiter**.

i. Klicken Sie im Fenster zur Auswahl des Zielverzeichnisses auf **Weiter**.

j. Klicken Sie im Fenster mit den ausgewählten Installationsoptionen auf **Weiter**.

k. Klicken Sie im nächsten Fenster auf **OK**, um mit der Installation des Produktes zu beginnen.

   Anmerkung: Die Ausführung dieses Schrittes kann mehrere Minuten dauern.

l. Klicken Sie im Fenster für den Installationsabschluss auf die Option für **Beenden**.

5. Geben Sie die folgenden Befehle ein, um den WebSphere-Datenträger abzuhängen. Wenn Sie diesen Befehl eingeben, kann kein Prozess auf Teile der Verzeichnisbaumstruktur von '/cdrom' zugreifen:

   ```
   cd /
   umount /cdrom
   ```

Nach Abschluss dieser Arbeitsschritte sind die folgenden Dateien installiert:

```
IBMWebAS.base.IBMApache    3.5.0.0  COMMITTED  IBMWebAS.base - IBMApache
IBMWebAS.base.ITJ.Info     1.0.0.0  COMMITTED  IBMWebAS.base - ITJ Info
IBMWebAS.base.WASicon      3.5.0.0  COMMITTED  IBMWebAS.base - WASicon
IBMWebAS.base.admin        3.5.0.0  COMMITTED  IBMWebAS.base - admin
IBMWebAS.base.samples      3.5.0.0  COMMITTED  IBMWebAS.base - samples
IBMWebAS.base.server       3.5.0.0  COMMITTED  IBMWebAS.base - server
IBMWebAS.base.tivoli       3.5.0.0  COMMITTED  IBMWebAS.base - tivoli
```

Upgrade für WebSphere Application Server ausführen

Gehen Sie wie folgt vor, um für WebSphere Application Server einen Upgrade auf die vorläufige Programmkorrektur (PTF) 4 durchzuführen:

1. Legen Sie die CD von *Tivoli PKI für AIX* in das CD-ROM-Laufwerk Ihres Systems ein. Geben Sie den folgenden Befehl ein, um die CD anzuhängen:

   ```
   mount /cdrom
   ```

2. Geben Sie den folgenden Befehl ein, um in das entsprechende Verzeichnis zu wechseln:

   ```
   cd /cdrom/aix/WebSphere-Standard-ptf4
   ```

3. Kopieren Sie alle WebSphere-PTF4-Dateien von der CD in ein Verzeichnis auf Ihrem System, auf das Sie über Root-Schreibberechtigung verfügen.

4. Geben Sie den folgenden Befehl ein, um das Script 'install.sh' auszuführen:

   ```
   ./install.sh
   ```

5. Geben Sie das WebSphere-Stammverzeichnis an, wenn Sie vom System hierzu aufgefordert werden. Standardmäßig wird als Stammverzeichnis /usr/WebSphere/AppServer verwendet.

6. Geben Sie auf die entsprechende Systemanfrage hin die Antwort ″**Ja**″ auf die Frage ein, ob Sie **IHS WebServer PTF installieren** wollen.

7. Geben Sie den Stammverzeichnispfad für das WebServer-Dokument an, wenn Sie vom System hierzu aufgefordert werden. Standardmäßig wird das Verzeichnis /usr/HTTPServer/htdocs/en_US verwendet. Bestätigen Sie die Auswahl durch Eingabe von ″**Ja**″.

Funktion für automatisches Starten des IBM HTTP Server inaktivieren

Zum Inaktivieren der Funktion für das automatische Starten des IBM HTTP Server-Dienstes müssen Sie mit Root-Berechtigung die folgenden Arbeitsschritte ausführen:

1. Geben Sie den folgenden Befehl ein, um in das Verzeichnis '/etc' zu wechseln:

   ```
   cd /etc
   ```

2. Editieren Sie die Datei inittab, und löschen Sie hierbei den Eintrag für **ihshttpd**. Speichern Sie die Datei 'inittab' nach dem Löschen des Eintrags.

3. Stoppen Sie den IBM HTTP Server-Dienst, der von WebSphere möglicherweise bereits gestartet wurde. Gehen Sie hierzu wie folgt vor:

   a. Geben Sie den folgenden Befehl ein, um die eventuell aktiven Prozesse aufzulisten:

      ```
      ps -ef | grep http
      ```

   b. Lokalisieren Sie den Prozess **/usr/HTTPServer/bin/httpd**.

   c. Suchen Sie die ID des Elternprozesses (zweites Feld von links).

   d. Stoppen Sie den Elternprozess mit dem Befehl **kill**. Beispiel:

      ```
      kill pid
      ```

      Hierbei steht *pid* für die ID des Elternprozesses.

WebSphere Application Server starten

Vor der Installation von Tivoli PKI müssen Sie WebSphere Application Server starten. Gehen Sie hierzu wie folgt vor:

1. Geben Sie den folgenden Befehl ein, um in das entsprechende Verzeichnis zu wechseln:

   ```
   cd /usr/WebSphere/AppServer/bin
   ```

2. Geben Sie den folgenden Befehl ein:

   ```
   ./startupServer.sh &
   ```

3. Geben Sie den folgenden Befehl ein, um in das entsprechende Verzeichnis zu wechseln:

   ```
   cd /usr/WebSphere/AppServer/logs
   ```

4. Geben Sie den folgenden Befehl ein, und überwachen Sie die Tracedatei:

```
tail -f tracefile
```

Wenn die Nachricht **A WebSphere Administration Server open for e-business** ausgegeben wird, wurde WebSphere Application Server gestartet.

Anmerkung: Die Ausführung dieses Schrittes kann mehrere Minuten dauern.

5. Drücken Sie die Tastenkombination **Strg + C**, um den Befehl **tail** zu beenden.

IBM 4758 PCI Cryptographic Coprocessor installieren

Sie müssen entscheiden, ob Sie die Einheit IBM 4758 zum Schutz von CA- und RA-Unterschriftsschlüsseln verwenden möchten. Wenn dies der Fall ist, müssen Sie die Hardware der Einheit IBM 4758 sowie das zugehörige Unterstützungsprogramm für die Verschlüsselung auf dem Server installieren, auf dem der Zertifikatsaussteller oder die Registrierungsstelle installiert werden soll. Befinden sich CA und RA auf der selben Maschine, kann der IBM 4758 PCI Cryptographic Coprocessor gemeinsam verwendet werden.

Informationen zum Installieren und Konfigurieren des IBM 4758 PCI Cryptographic Coprocessor finden Sie in der Produktdokumentation zur Einheit IBM 4758

Tivoli PKI installieren

Vor dem Installieren von Tivoli PKI sollten Sie unbedingt die neueste Version der Release-Informationen für das Produkt lesen. Die aktuellste Version dieses Dokuments können Sie über die Website von Tivoli PKI abrufen.

Verwenden Sie die folgenden Richtlinien, um die Produktkomponenten von Tivoli PKI zu installieren:

- Installieren Sie alle Serverprogramme auf der selben Plattform (im vorliegenden Fall also unter AIX).

- Wurde zuvor IBM KeyWorks Version 1.1.1 installiert, müssen Sie Tivoli PKI entweder auf einer anderen Maschine installieren oder die KeyWorks-Software und alle zugehörigen Anwendungen entfernen, bevor Sie das Installationsprogramm von Tivoli PKI starten.
- Wenn Sie Tivoli PKI in einer Konfiguration mit mehreren Maschinen installieren wollen, müssen Sie die Installationsprozeduren auf den gewünschten Maschinen wiederholen, bis alle Serverkomponenten installiert sind. Weitere Informationen hierzu finden Sie im Abschnitt „Richtlinien für die Installation auf mehreren Maschinen" auf Seite 82.
- Wenn Sie das RA Desktop-Applet installieren wollen, müssen Sie zuerst ein Installationsimage installieren. Anschließend muss das Image verteilt oder über das Netz zur Verfügung gestellt werden, damit die Benutzer das Installationsprogramm über eine lokale Windows-Maschine ausführen können. Instruktionen zum Installieren, Konfigurieren und Deinstallieren dieser Programme finden Sie in der Veröffentlichung *Tivoli PKI RA Desktop*.
- Wenn Sie das System nach der Installation der Softwarevoraussetzungen nicht erneut gestartet haben, müssen Sie jetzt einen Neustart durchführen. Stellen Sie sicher, dass die Umgebungsvariablen korrekt definiert sind, bevor Sie Tivoli PKI installieren.
- Verwenden Sie PING oder ein anderes Netzkonnektivitäts-Tool, um zu überprüfen, ob die Hostnamen und IP-Adressen gültig und auf dem DNS-Server (DNS = Domain Name Services) Ihres Netzes definiert sind.

KeyWorks installieren

Gehen Sie wie folgt vor, um IBM KeyWorks zu installieren:

1. Melden Sie sich als Benutzer mit Root-Berechtigung an.
2. Legen Sie die CD von *Tivoli PKI für AIX* in das CD-ROM-Laufwerk Ihres Systems ein. Geben Sie den folgenden Befehl ein, um die CD anzuhängen:

   ```
   mount /cdrom
   ```

3. Geben Sie den folgenden Befehl ein, um in das entsprechende Verzeichnis zu wechseln:

```
cd /cdrom/kw
```

4. Geben Sie den folgenden Befehl ein, um KeyWorks zu installieren:

   ```
   smitty install_latest
   ```

5. Wählen Sie für die Option **EINGABE-Einheit/Verzeichnis für Software .** (Punkt) aus.

6. Drücken Sie unter **Neueste verfügbare Software installieren und aktualisieren** die **Eingabetaste**.

7. Wenn Sie mit der Installation von Tivoli PKI fortfahren, können Sie diesen Arbeitsschritt überspringen. Andernfalls müssen Sie den folgenden Befehl eingeben, um das CD-ROM-Laufwerk abzuhängen:

   ```
   umount /cdrom
   ```

Nach Abschluss dieser Arbeitsschritte sind die folgenden Dateien installiert:

```
sway.adt            1.1.3.1  COMMITTED  IBM KeyWorks
sway_vr.cst         1.1.3.1  COMMITTED  Domestic (US) customization
```

Serversoftware installieren

Gehen Sie wie folgt vor, um die Serversoftware zu installieren:

1. Melden Sie sich als Benutzer mit Root-Berechtigung an.

2. Legen Sie die CD von *Tivoli PKI für AIX* in das CD-ROM-Laufwerk ein. Geben Sie den folgenden Befehl ein, um die CD anzuhängen:

   ```
   mount /cdrom
   ```

3. Geben Sie den folgenden Befehl ein, um in das entsprechende Verzeichnis zu wechseln:

   ```
   cd /cdrom/usr/sys/inst.images
   ```

4. Geben Sie den folgenden Befehl ein:

   ```
   smitty
   ```

5. Wählen Sie **Softwareinstallation und Wartung** aus.

6. Wählen Sie **Software installieren und aktualisieren** aus.

7. Wählen Sie **Neueste verfügbare Software installieren und aktualisieren** aus.
8. Wählen Sie für die Option **EINGABE-Einheit/Verzeichnis für Software .** (Punkt) aus.
9. Drücken Sie unter **SOFTWARE, die installiert werden soll** die Taste **F4**, um eine Liste der Dateien anzuzeigen, die für die Installation zur Verfügung stehen.
10. Verwenden Sie die folgende Tabelle als Richtlinie und wählen Sie die Komponente oder Komponenten aus, die Sie auf dieser Maschine installieren möchten; drücken Sie anschließend die Eingabetaste.

    Die Datei 'ta.doc' enthält HTML-Hilfedateien und die Tivoli PKI-Dokumentation für die folgenden Bereiche:
    - *Tivoli PKI-Konfiguration*
    - *Tivoli PKI Registration Authority Desktop*

    Die Datei 'ta.srvr' enthält Folgendes:
    - Unterstützung für IBM 4758 PCI Cryptographic Coprocessor
    - Zertifikatsaussteller (CA = Certificate Authority)
    - Kerndateien
    - Grafische Benutzerschnittstelle (GUI) für die Installation
    - Installations-Tools
    - Registrierungsstelle (RA = Registration Authority)

    Anmerkung: Die Option für die Unterstützung des IBM 4758 PCI Cryptographic Coprocessor darf nicht ausgewählt werden, wenn auf der verwendeten Maschine diese Einheit nicht installiert ist. Mit der Taste **F7** können Sie die zu installierenden Dateien auswählen.

Dateiname	Komponente	Beschreibung
tpki.srvr.ra	RA-Server	Installation der RA-Serversoftware, einschließlich aller Dateien, die für die Registrierungsfunktion erforderlich sind.

Dateiname	Komponente	Beschreibung
tpki.srvr.ca	CA- und Prüfserver	Installation der CA- und Prüfsubsystemprogramme.
tpki.srvr.core	Tivoli PKI	Installation der wichtigsten Tivoli PKI-Bibliotheken.
tpki.srvr.ic	Installations-Tools	Installation der Installations-Tools von Tivoli PKI.
tpki.srvr.icg	Grafische Benutzer-schnittstelle (GUI) für die Installation	Installation der grafischen Installationsbenutzerschnittstelle (GUI) von Tivoli PKI.
RADInst.exe	RA Desktop	Installation eines Installations-Images für das RA Desktop-Applet von Tivoli PKI (nur Windows NT).

11. Nach Beendigung dieser Arbeitsschritte ist die Tivoli PKI-Installation abgeschlossen. Geben Sie die folgenden Befehle ein, um das CD-ROM-Laufwerk abzuhängen:

```
cd /
umount /cdrom
```

Nach Abschluss dieser Arbeitsschritte sind die folgenden Dateien installiert:

```
tpki.srvr.ca                3.7.1.0  COMMITTED  IBM Trust Authority
tpki.srvr.core              3.7.1.0  COMMITTED  IBM Trust Authority
                                                          Core Files
tpki.srvr.ic                3.7.1.0  COMMITTED  IBM Trust Authority
tpki.srvr.icg               3.7.1.0  COMMITTED  IBM Trust Authority
tpki.srvr.ra                3.7.1.0  COMMITTED  IBM Trust Authority
tpki.doc.cfg                3.7.1.0  COMMITTED  IBM Trust Authority
                                                           Config
tpki.doc.rad                3.7.1.0  COMMITTED  IBM Trust Authority
                                                         RA Desktop
tpki.doc.usr                3.7.1.0  COMMITTED  IBM Trust User Guide
```

Richtlinien für die Installation auf mehreren Maschinen

Im vorliegenden Abschnitt werden die Richtlinien erläutert, die bei der Installation von Tivoli PKI in einer Konfiguration mit mehreren Maschinen berücksichtigt werden müssen. Hierbei werden die folgenden Konfigurationen erläutert:

- Szenario 1 - RA-Server auf einer Maschine; CA-, Prüf- und Directory-Server auf einer anderen Maschine
- Szenario 2 - RA- und Directory-Server auf einer Maschine; CA- und Prüfserver auf einer anderen Maschine
- Szenario 3 - RA-, Prüf- und CA-Server auf einer Maschine; Directory-Server auf einer anderen Maschine
- Szenario 4 - RA-Server auf einer Maschine; CA- und Prüfserver auf einer anderen Maschine; Directory-Server auf einer dritten Maschine

Verwenden Sie die folgenden Installationsrichtlinien gemäß den Anforderungen Ihrer Tivoli PKI-Maschinenkonfiguration.

Szenario 1 - RA-Server auf einer Maschine; CA-, Prüf- und Directory-Server auf einer anderen Maschine

Für den RA-Server müssen folgende Softwarekomponenten installiert bzw. folgende Arbeitsschritte ausgeführt werden:

- AIX 4.3.3.0
- AIX 4.3.3.0 Wartungsstufe 6
- IBM DB2 Universal Database Version 6.1 Fix Pack 4
- IBM Directory Client
- IBM Developer Kit für AIX, Java Technology Edition, Version 1.2.2 PTF 8
- IBM WebSphere Application Server Standard Edition Version 3.5
- Führen Sie einen Upgrade von IBM WebSphere Application Server Standard Edition auf Version 3.5 PTF 4 aus.
- Inaktivieren Sie die Funktion für automatisches Starten des IBM HTTP Server.
- Starten Sie WebSphere Application Server.

- IBM Key Works
- Tivoli PKI-Dateien: tpki.srvr.core, tpki.srvr.ic, tpki.srvr.icg, tpki.srvr.ra

Für den CA-, Prüf- und Directory-Server müssen folgende Softwarekomponenten installiert werden:

- AIX 4.3.3.0
- AIX 4.3.3.0 Wartungsstufe 6
- IBM DB2 Universal Database Version 6.1 Fix Pack 4
- IBM Directory Server Version 3.1.1.5
- IBM Developer Kit für AIX, Java Technology Edition, Version 1.2.2 PTF 8
- IBM Key Works
- Tivoli PKI-Dateien: tpki.srvr.core, tpki.srvr.ic, tpki.srvr.ca

Szenario 2 - RA- und Directory-Server auf einer Maschine; CA- und Prüfserver auf einer anderen Maschine

Für den RA- und Directory-Server müssen folgende Softwarekomponenten installiert bzw. folgende Arbeitsschritte ausgeführt werden:

- AIX 4.3.3.0
- AIX 4.3.3.0 Wartungsstufe 6
- IBM DB2 Universal Database Version 6.1 Fix Pack 4
- IBM Directory Server Version 3.1.1.5
- IBM Developer Kit für AIX, Java Technology Edition, Version 1.2.2 PTF 8
- IBM WebSphere Application Server Standard Edition Version 3.5
- Führen Sie einen Upgrade von IBM WebSphere Application Server Standard Edition auf Version 3.5 PTF 4 aus.
- Inaktivieren Sie die Funktion für automatisches Starten des IBM HTTP Server.
- Starten Sie WebSphere Application Server.
- IBM Key Works
- Tivoli PKI-Dateien: tpki.srvr.core, tpki.srvr.ic, tpki.srvr.icg, tpki.srvr.ra

Für den CA- und Prüfserver müssen folgende Softwarekomponenten installiert werden:

- AIX 4.3.3.0
- AIX 4.3.3.0 Wartungsstufe 6
- IBM DB2 Universal Database Version 6.1 Fix Pack 4
- IBM Directory Client
- IBM Developer Kit für AIX, Java Technology Edition, Version 1.2.2 PTF 8
- IBM Key Works
- Tivoli PKI-Dateien: tpki.srvr.core, tpki.srvr.ic, tpki.srvr.ca

Szenario 3 - RA-, Prüf- und CA-Server auf einer Maschine; Directory-Server auf einer anderen Maschine

Für den RA-, Prüf- und CA-Server müssen folgende Softwarekomponenten installiert bzw. folgende Arbeitsschritte ausgeführt werden:

- AIX 4.3.3.0
- AIX 4.3.3.0 Wartungsstufe 6
- IBM DB2 Universal Database Version 6.1 Fix Pack 4
- IBM Directory Client
- IBM Developer Kit für AIX, Java Technology Edition, Version 1.2.2 PTF 8
- IBM WebSphere Application Server Standard Edition Version 3.5
- Führen Sie einen Upgrade von IBM WebSphere Application Server Standard Edition auf Version 3.5 PTF 4 aus.
- Inaktivieren Sie die Funktion für automatisches Starten des IBM HTTP Server.
- Starten Sie WebSphere Application Server.
- IBM Key Works
- Tivoli PKI-Dateien: tpki.srvr.core, tpki.srvr.ic, tpki.srvr.icg, tpki.srvr.ra, tpki.srvr.ca

Für den Directory-Server müssen folgende Softwarekomponenten installiert werden:

- AIX 4.3.3.0
- AIX 4.3.3.0 Wartungsstufe 6
- IBM DB2 Universal Database Version 6.1 Fix Pack 4
- IBM Directory Server Version 3.1.1.5
- IBM Developer Kit für AIX, Java Technology Edition, Version 1.2.2 PTF 8

- IBM Key Works
- Tivoli PKI-Dateien: tpki.srvr.core, tpki.srvr.ic

Szenario 4 - RA-Server auf einer Maschine; CA- und Prüfserver auf einer anderen Maschine; Directory-Server auf einer dritten Maschine

Für den RA-Server müssen folgende Softwarekomponenten installiert bzw. folgende Arbeitsschritte ausgeführt werden:

- AIX 4.3.3.0
- AIX 4.3.3.0 Wartungsstufe 6
- IBM DB2 Universal Database Version 6.1 Fix Pack 4
- IBM Directory Client
- IBM Developer Kit für AIX, Java Technology Edition, Version 1.2.2 PTF 8
- IBM WebSphere Application Server Standard Edition Version 3.5
- Führen Sie einen Upgrade von IBM WebSphere Application Server Standard Edition auf Version 3.5 PTF 4 aus.
- Inaktivieren Sie die Funktion für automatisches Starten des IBM HTTP Server.
- Starten Sie WebSphere Application Server.
- IBM Key Works
- Tivoli PKI-Dateien: tpki.srvr.core, tpki.srvr.ic, tpki.srvr.icg, tpki.srvr.ra

Für den CA- und Prüfserver müssen folgende Softwarekomponenten installiert werden:

- AIX 4.3.3.0
- AIX 4.3.3.0 Wartungsstufe 6
- IBM DB2 Universal Database Version 6.1 Fix Pack 4
- IBM Directory Client
- IBM Developer Kit für AIX, Java Technology Edition, Version 1.2.2 PTF 8
- IBM Key Works
- Tivoli PKI-Dateien: tpki.srvr.core, tpki.srvr.ic, ta.srvr.ca

Für den Directory-Server müssen folgende Softwarekomponenten installiert werden:

- AIX 4.3.3.0

- AIX 4.3.3.0 Wartungsstufe 6
- IBM DB2 Universal Database Version 6.1 Fix Pack 4
- IBM Directory Server Version 3.1.1.5
- IBM Developer Kit für AIX, Java Technology Edition, Version 1.2.2 PTF 8
- IBM Key Works
- Tivoli PKI-Dateien: tpki.srvr.core, tpki.srvr.ic

Bootwerte ändern

Verwenden Sie diese Prozedur nur, wenn Sie einen der standardmäßigen Konfigurationswerte ändern wollen. Hierbei handelt es sich um die Werte, die bei der Ausführung des Konfigurations-Applets oder nach der Konfiguration des Systems nicht geändert werden können. Sie müssen alle Boot-Änderungen vornehmen, bevor Sie das Tivoli PKI-Konfigurationsprogramm für den Installationsabschluss ausführen. Wenn die Bootwerte nicht geändert werden sollen, können Sie mit Abschnitt „Konfigurationsprogramm für den Installationsabschluss ausführen" auf Seite 90 fortfahren.

Tivoli PKI führt im Rahmen des Installationsabschlussprozesses ein Boot-Programm aus. Als Eingabe für dieses Boot-Programm wird ein SQL-Script mit dem Namen 'createconfig_start.sql' verwendet, das Standardwerte in die Konfigurationsdatenbank lädt und in der Datenbanktabelle 'ConfigDataTbl' Definitionen für Datenbanktabellen erstellt. Diese Tabelle enthält die Daten für die Systemkonfiguration aller Tivoli PKI-Komponenten. Verschiedene Werte in diesem SQL-Script können nach dem Starten des Konfigurationsprozesses nicht mehr geändert werden.

Anmerkung: In kritischen Situationen, in denen ein Standardwert zu Problemen in der Betriebsumgebung führen würde, können Sie vor der Konfiguration auch die Schablonendateien von Tivoli PKI ändern. Wenn Sie weitere Informationen hierzu benötigen, wenden Sie sich bitte an den zuständigen IBM Ansprechpartner.

Wenn Sie einen Boot-Wert ändern wollen, müssen Sie die Datei 'createconfig_start.sql' editieren. Diese Datei wird standardmäßig im Verzeichnis '/usr/lpp/iau/bin' gespeichert.

Verwenden Sie die folgende Tabelle als Richtlinie für die Durchführung von Änderungen:

- Wenn Sie den Wert von DATABASE PATHNAME ändern wollen, müssen Sie den vollständigen Pfad für die neue Adresse angeben. Beispiel: /local/dbfsibm.
- Die registrierten Namen (DNs) für die Tivoli PKI-Registrierungsstelle, den Directory-Administrator und das Prüfsubsystem sind für den Benutzer transparent. Wenn Sie diese ändern wollen, müssen Sie darauf achten, dass nur das Attribut für den allgemeinen Namen (CN) geändert wird. Der DN-Basiswert für den Zertifikatsaussteller (CA), den Sie während der Konfiguration angegeben haben, wird auch für den von Ihnen ausgewählten allgemeinen Namen (CN) angewendet.

Feldname	Beschreibung	Standardwert
WS_RO_KEYSIZE	Schlüsselgröße für den Schlüsselring des Web-Servers. Die Optionen 0 - 3, die in der KeySize-Aufzählung definiert sind, sind wie folgt zugeordnet: ■ 0 = 512 ■ 1 = 768 ■ 2 = 1024 ■ 3 = 2048	0
DATABASE _PATHNAME	Der vollständig qualifizierte Pfad für die Adresse, an der das Exemplar der CA-Datenbank (die CA-Komponente) physisch gespeichert ist.	dbfsibm

Feldname	Beschreibung	Standardwert
DATABASE _PATHNAME	Der vollständig qualifizierte Pfad für die Adresse, an der das Exemplar der Prüfdatenbank (die Prüfsubsystemkomponente) physisch gespeichert ist.	dbfsadt
DATABASE _PATHNAME	Der vollständig qualifizierte Pfad für die Adresse, an der das Exemplar der Registrierungsdatenbank (die RA-Komponente) physisch gespeichert ist.	dbfspkrf
APP_DN	Der registrierte Name (DN) der Registrierungsstelle (RA) von Tivoli PKI. Sie können lediglich den allgemeinen Namen (CN) ändern.	/C=US/O=Ihr Unternehmen/OU=Tivoli PKI/CN=Tivoli PKI-RA
APP_CERT _LIFETIME	Die in Monaten angegebene Lebensdauer der RA-Zertifikate eines Systems.	36 Dieser Wert muss ein Mehrfaches von 12 sein.
APP_LDAP _DIR ADMIN_DN	Der registrierte Name (DN) des Directory-Administrators. Sie können lediglich den allgemeinen Namen (CN) ändern.	/C=US/O=Ihr Unternehmen/OU=Tivoli PKI/CN=DirAdmin

Feldname	Beschreibung	Standardwert
APP_COMM _PORT	Der Kommunikations-Port, der zur Durchführung der Kommunikation zwischen dem Gerüst der Registrierungsfunktion und der Registrierungsstelle von Tivoli PKI verwendet wird.	29783
APP_SEC_MECH	Der Sicherheitsmechanismus der Anwendung. Standardmäßig wird die RA-Datenbankverschlüsselung inaktiviert. Wenn Sie den Wert auf 1 setzen, wird die Datenbankverschlüsselung aktiviert.	0
CA_IBM_CA_CERT _LIFETIME	Die in Monaten angegebene Lebensdauer des CA-Zertifikats von Tivoli PKI.	36 Dieser Wert muss ein Mehrfaches von 12 sein.
CA_IBM_ADMIN _PORT	Der Verwaltungs-Port des Zertifikatsausstellers (CA) von Tivoli PKI. Der angegebene Wert muss auch für den PORT-Eintrag in der Datei (irgAutoCA.ini.tpl) definiert werden, die im Verzeichnis 'cfg' gespeichert ist.	1835

Feldname	Beschreibung	Standardwert
ADT_DN	Der registrierte Name (DN) des Prüfsubsystems. Sie können lediglich den allgemeinen Namen (CN) ändern.	/C=US/O=Ihr Unternehmen/OU=Tivoli PKI/CN=Tivoli PKI-Prüfsubsystem

Konfigurationsprogramm für den Installationsabschluss ausführen

Nach der Installation der Tivoli PKI-Serversoftware müssen Sie das Konfigurationsprogramm 'CfgPostInstall' für den Installationsabschluss auf dem Tivoli PKI-Hauptserver ausführen, auf dem die RA, WebSphere sowie der HTTP-Server installiert sind. Sie müssen dieses Programm ausführen, bevor Sie Tivoli PKI mit dem Setup Wizard konfigurieren.

Von diesem Programm wird eine Webserver-Konfigurationsdatei (httpd.conf) erstellt, die das Starten des Webservers mit den für Tivoli PKI erforderlichen Parametern ermöglicht. Es bereitet darüber hinaus den Web-Server für die Ausführung des Konfigurations-Applets vor, erstellt einen Benutzereintrag für die Tivoli PKI-Konfiguration (cfguser) sowie die Konfigurationsdatenbank und füllt die Datenbank mit den Standardkonfigurationsdaten.

Gehen Sie wie folgt vor, um das Konfigurationsprogramm für den Installationsabschluss auszuführen:

1. Melden Sie sich als Root an, und geben Sie hierzu den folgenden Befehl ein:

   ```
   su - root
   ```

2. Geben Sie den folgenden Befehl ein, um in das entsprechende Verzeichnis zu wechseln:

   ```
   cd /usr/lpp/iau/bin
   ```

3. Geben Sie den folgenden Befehl ein:

   ```
   ./CfgPostInstall -i
   ```

4. Definieren Sie, wenn Sie vom System hierzu aufgefordert werden, das Kennwort für den Benutzereintrag 'cfguser' und bestätigen Sie dieses.
5. Definieren Sie, wenn Sie vom System hierzu aufgefordert werden, das Kennwort für das Steuerprogramm und bestätigen Sie dieses.
6. Wählen Sie als Name für das DB2-Exemplar 'db2inst1' aus. Geben Sie den Wert **1** ein, der dem Namen 'db2inst1' zugeordnet ist.

Anmerkung: Die Ausführung dieses Schrittes kann mehrere Minuten dauern.

Prüfliste für den Installationsabschluss

Verwenden Sie die folgenden Prüfliste, um sicherzustellen, dass alle Voraussetzungen erfüllt sind, um mit der Konfiguration von Tivoli PKI zu beginnen. Informationen zum Ausführen des Setup Wizard finden Sie im Handbuch *Tivoli PKI Konfiguration*.

1. Melden Sie sich mit Root-Berechtigung an und geben Sie anschließend die folgenden Befehle ein, um eine Sicherungskopie des System-Images zu erstellen:

   ```
   smitty mksysb
   smitty savevg
   ```

2. Erstellen Sie zur Unterstützung bei der späteren Fehlerbehebung eine Liste der gesamten Software, die auf den einzelnen Servern installiert ist. Melden Sie sich mit Root-Berechtigung an und geben Sie anschließend den folgenden Befehl ein:

   ```
   #lslpp -al >tmp/sys_software.txt
   ```

3. Wenn Sie nicht beabsichtigen, die Standardkonfigurationswerte für Web-Server-Ports zu verwenden, müssen Sie die IP-Aliasnamen konfigurieren, bevor Sie den Setup Wizard ausführen. Die Konfigurationsprogramme verwenden diese Werte bei der Erstellung des CA-Zertifikats für Ihr System. Informationen dazu, wie Tivoli PKI Ports auf dem Web-Server konfiguriert und verwendet, um gesicherte und nicht gesicherte Transaktionen zu verarbeiten, finden Sie in „IP-Aliasnamen für den Webserver konfigurieren" auf Seite 44.

4. Entscheiden Sie, welche registrierten Namen (DN) für den Tivoli PKI-CA und die zugehörigen Agenten, den Directory-Administrator und den Directory-Root verwendet werden sollen. Diese registrierten Namen (DNs) müssen eindeutig sein.

   Prüfen Sie die Richtlinien im Handbuch *Tivoli PKI Konfiguration*, um sicherzustellen, dass die registrierten Namen (DNs) für diese Objekte die gewünschte Zertifizierungshierarchie auch unterstützen.

5. Füllen Sie das *Tivoli PKI-Konfigurationsdatenformular* aus, das im Handbuch *Tivoli PKI Konfiguration* enthalten ist, um sich mit den Informationen vertraut zu machen, die Sie für die Konfiguration des Systems bereithalten müssen. Verwenden Sie dieses Formular, um Informationen zum jeweiligen System aufzuzeichnen, wie beispielsweise die Server-Host-Namen und die bevorzugten registrierten Namen (DN).

Backup-Dienstprogramm ausführen

Das Backup-Dienstprogramm von Tivoli PKI (ta-backup) ist ein Tool zum Sichern von Konfigurationsdaten, die in keiner der DB2-Datenbanken gespeichert sind. Die zugehörigen Dateiinformationen wie z. B. Dateiberechtigungen etc. werden ebenfalls gesichert. Verwenden Sie zum Sichern von DB2-Datenbanken die entsprechenden DB2-Dienstprogramme.

Das Backup-Dienstprogramm akzeptiert einen Parameter, der das Verzeichnis angibt, in das Backup-Daten geschrieben werden sollen. Dieses Backup-Verzeichnis ist das Stammverzeichnis, das zum Speichern aller Datendateien eingesetzt wird. Um Namensunverträglichkeiten innerhalb des Backup-Verzeichnisses zu verhindern, speichert das Backup-Dienstprogramm Dateien mit derselben Verzeichnisstruktur, die auch auf dem gesicherten System definiert wurde.

Das folgende Beispiel illustriert die Programmsyntax:

```
ta-backup -d backup_directory
```

Hierbei steht *backup_directory* für das Verzeichnis, das für die Datensicherung verwendet werden soll. Der Standardpfad lautet '/usr/lpp/iau/backup'.

Führen Sie die folgenden Arbeitsschritte aus, um das Dienstprogramm 'ta-backup' im Offline-Modus auszuführen:

1. Melden Sie sich als Benutzer mit Root-Berechtigung an.
2. Erstellen Sie optional das Backup-Verzeichnis für die Tivoli PKI-Konfigurationsdaten. Beispiel:

   ```
   mkdir /usr/lpp/iau/my_tabackup
   ```

3. Wechseln Sie in das Verzeichnis 'bin' von Tivoli PKI. Der Standardpfad lautet '/usr/lpp/iau/bin'.
4. Geben Sie den folgenden Befehl ein, um zu definieren, wo die Daten gesichert werden sollen:

   ```
   ta-backup -d /usr/lpp/iau/my_tabackup
   ```

5. Geben Sie nach einer entsprechenden Systemanfrage das Kennwort des Steuerprogramms an.

5

Tivoli PKI unter Windows NT installieren

Das vorliegende Kapitel enthält Prozeduren zum Installieren von Tivoli Public Key Infrastructure (PKI) sowie der für den Betrieb erforderlichen Produkte auf einer Windows NT-Plattform.

Anmerkung: Tivoli PKI Version 3.7.1 bietet keine Unterstützung für Windows NT. Diese Informationen wurden nur zu Referenzzwecken aufgeführt.

Vor dem Installieren der Tivoli PKI-Software sollten Sie unbedingt die neueste Version der Release-Informationen für das Produkt lesen. Die aktuellste Version dieses Dokuments können Sie über die Website von Tivoli Public Key Infrastructure abrufen.

Anmerkung: Bei den wichtigsten Prozeduren in diesem Kapitel wird davon ausgegangen, dass Sie Tivoli PKI zum ersten Mal installieren. Vor der Installation von Tivoli PKI sollten Sie unbedingt eine Sicherungskopie Ihrer Datendateien erstellen. Informationen zur Erstellung von Sicherungskopien für Ihre Datendateien finden Sie im Abschnitt „Backup-Dienstprogramm ausführen” auf Seite 117. Führen Sie nach dem Backup über die Befehlszeile das Programm ’CfgUnInstall’ aus, und setzen Sie anschließend die Installation von Tivoli PKI fort.

Installieren Sie die Software für Tivoli PKI in der folgenden Reihenfolge:

1. Betriebssystem Microsoft Windows NT, Version 4.0 mit Service Pack 5.
2. Tivoli PKI-Datenbank-Software (IBM DB2 Universal Database für Tivoli PKI).
3. Sun Java Development Kit (JDK) ab Version 1.1.6.
4. IBM HTTP Server (IHS) Version 1.3.3.1 einschließlich Global Services Kit (GSK).
5. IBM WebSphere Application Server Version 2.0.3.1.
6. IBM Directory Server Version 3.1.1
7. Tivoli PKI-Serversoftware einschließlich der zentralen Serverprogramme und Installations-Images für die Client-Anwendung und RA Desktop.

Konfiguration mit mehreren Maschinen

Wenn nicht die gesamte Server-Software auf einer Maschine installiert werden soll, müssen Sie die folgenden Prozeduren zur Installation von Windows NT und der Datenbanksoftware von Tivoli PKI auf allen beteiligten Maschinen wiederholen.

Windows NT konfigurieren

Gehen Sie anhand der folgenden Richtlinien vor, wenn Sie die Windows NT-Software auf der Maschine bzw. den Maschinen installieren, auf der/denen die Tivoli PKI-Software installiert werden soll. Wenn Sie Windows NT bereits installiert haben, können Sie diese Richtlinien als Prüfliste verwenden, um sicherzustellen, dass alle Dateien installiert wurden, die für die Tivoli PKI-Komponenten erforderlich sind.

Wenn Sie Tivoli PKI in einer Konfiguration mit mehreren Maschinen installieren wollen, müssen Sie auf allen Maschinen, auf denen eine Serverkomponente von Tivoli PKI installiert werden soll, zuerst Windows NT installieren.

- Bei der Installation von Windows NT müssen Sie auch das Protokoll TCP/IP installieren. DHCP (Dynamic Host Configuration Protocol) kann nur verwendet werden, wenn Sie über einen dynamischen DNS-Server (DNS = Domain Name Services) verfügen.
- Verwenden Sie die folgenden Richtlinien, um die Konnektivität zu aktivieren:
  - Prüfen Sie, ob die IP-Adressen und Host-Namen zugeordnet und fest definiert sind.
  - Prüfen Sie, ob Sie über IP-Konnektivität verfügen. Hierzu können Sie z. B. feststellen, ob Sie ein PING-Signal an eine andere Maschine absetzen können.
  - Prüfen Sie, ob DNS und die zugehörige Umkehrfunktion korrekt arbeiten. Hierzu können Sie z. B. feststellen, ob der Befehl **`ping`** ***`hostname`*** in die korrekte IP-Adresse und der Befehl **`ping -a`** ***`IPaddress`*** in den korrekten Host-Namen aufgelöst wird.
- Prüfen Sie, ob auf der Maschine ein Verzeichnis 'temp' definiert wurde. Falls dies nicht der Fall ist, müssen Sie dieses Verzeichnis erstellen. Geben Sie den Befehl **`md %temp%`** ein, um zu prüfen, ob das Verzeichnis 'temp' vorhanden ist oder um dieses zu erstellen. Wenn das Verzeichnis bereits vorhanden ist, gibt das System eine Nachricht aus, in der Sie darüber informiert werden, dass ein entsprechendes Unterverzeichnis bzw. eine entsprechende Datei bereits existiert. Andernfalls erstellt das System das Verzeichnis 'temp'.
- Definieren Sie für den virtuellen Speicher der Maschine mindestens 400 MB und gehen Sie hierzu wie folgt vor:
  1. Wählen Sie **Start → Einstellungen → Systemsteuerung** aus.
  2. Klicken Sie **System** doppelt an und wählen Sie anschließend die Indexzunge **Leistungsmerkmale** aus.

3. Klicken Sie im Bereich **Virtueller Arbeitsspeicher** auf **Ändern**.
4. Ändern Sie den Wert für **Anfangsgröße** auf 400 MB und den Wert für **Maximale Größe** auf 500 MB.
5. Klicken Sie auf **Setzen**.
6. Klicken Sie auf **OK**, um das Dialogfenster zu schließen.
7. Klicken Sie auf **OK**, um das Fenster 'Systemeigenschaften' zu schließen.
8. Klicken Sie auf **Ja**, um einen Neustart des Computers durchzuführen.

- Erstellen Sie einen Windows NT-Benutzereintrag, der als Eintrag für den Tivoli PKI-Konfigurationsbenutzer eingesetzt werden kann. Die Konfigurationsprogramme verwenden diesen Benutzernamen und das zugehörige Kennwort, um die erforderlichen Datenbanken zu erstellen und das System zu konfigurieren. Verwenden Sie die Verwaltungs-Tools von Windows NT, um diesen Benutzereintrag wie folgt zu definieren:
  1. Führen Sie in der Programmgruppe der Verwaltungs-Tools das Programm **Benutzer-Manager** aus.
  2. Fügen Sie den Benutzereintrag **cfguser** hinzu, und kopieren Sie hierzu den Benutzereintrag für den Administrator (indem Sie diesen hervorheben und anschließend die Taste **F8** drücken). Der Benutzer muss über Administratorberechtigungen für Windows NT verfügen.
  3. Geben Sie ein Kennwort für 'cfguser' ein, und bestätigen Sie dieses, indem Sie es erneut eingeben.
  4. Nehmen Sie die Auswahl von **Benutzer muss Kennwort bei nächster Anmeldung ändern** zurück.
  5. Klicken Sie auf **OK**.

     Das Kennwort, das diesem Benutzernamen zugeordnet ist, muss genau 8 Zeichen lang sein. Um die Sicherheitsvorkehrungen zu optimieren, sollte eine Zeichenfolge angegeben werden, die kein tatsächliches Wort darstellt. Das Kennwort

sollte darüber hinaus eine Mischung aus Groß- und Kleinbuchstaben und mindestens eine Zahl enthalten.

- Diesen Benutzernamen und das zugehörige Kennwort müssen Sie bei der Installation und Konfiguration des Systems angeben; möglicherweise ist er auch für die Ausführung bestimmter Systemverwaltungs-Tools in Tivoli PKI erforderlich.
- Wenn Sie Tivoli PKI in einer Konfiguration mit mehreren Maschinen installieren wollen, müssen Sie den selben Benutzernamen sowie das zugehörige Kennwort auf allen Maschinen erstellen.

Sie sollten vor der Fortsetzung der Tivoli PKI-Installation Ihr Windows NT-System sichern. Mit Hilfe eines Sicherungs-Images kann das System wiederhergestellt werden, falls Probleme auftreten.Sie können das Sicherungsprogramm verwenden, das über die Verwaltungs-Tools von Windows NT zur Verfügung steht, um ein System-Image zu erstellen. Alternativ dazu können Sie auch ein anderes, mit Windows kompatibles Sicherungsprogramm verwenden.

Datenbanksoftware installieren

Tivoli PKI verwendet zum Verwalten von Daten IBM DB2 Universal Database. Die Software, die zum Lieferumfang von Tivoli PKI gehört, darf nur zusammen mit Tivoli PKI-Anwendungen eingesetzt werden. Wenn Sie die Datenbanksoftware anpassen oder zusammen mit anderen Anwendungen als Tivoli PKI verwenden wollen, müssen Sie eine Lizenz für eine Vollversion von IBM DB2 Enterprise Edition, Version 5.2 kaufen und anschließend das Fix-Pack 10 anwenden.

Führen Sie die nachfolgend beschriebene Prozedur aus, um die Datenbanksoftware zu installieren. Wenn Sie Tivoli PKI in einer Konfiguration mit mehreren Maschinen installieren wollen, müssen Sie auf allen Maschinen, auf denen eine Server-Komponente von Tivoli PKI installiert werden soll, zuerst die Datenbanksoftware installieren.

1. Legen Sie die CD von *Tivoli Public Key Infrastructure für NT* in das CD-ROM-Laufwerk ein.
2. Wählen Sie **Start → Ausführen** aus.
3. Klicken Sie auf **Durchsuchen**, um zum CD-ROM-Laufwerk zu wechseln.
4. Führen Sie die Datei **`setup.exe`** aus.
5. Wählen Sie im Fenster für die Auswahl der Setup-Sprache eine Sprache für die aktuelle Installation aus, und klicken Sie dann auf **OK**.
6. Lesen Sie die Informationen im Eingangsfenster und klicken Sie anschließend auf **Weiter**.

   Anmerkung: Wurde auf der Maschine bereits DB2 in der korrekten Version installiert, ruft das Programm das Fenster 'Setup abgeschlossen' auf. Klicken Sie im Fenster auf **Beenden**, um die Installation abzuschließen.
7. Klicken Sie im Fenster 'Zielpfad wählen' auf **Weiter**, wenn Sie den Standardinstallationspfad verwenden wollen. Wählen Sie andernfalls das gewünschte Laufwerk und den gewünschten Zielordner aus, in dem die Software installiert werden soll, und klicken Sie anschließend auf **Weiter**. (Im vorliegenden Fall kann der Standardpfad 'c:\Program Files\IBM\Trust Authority' verwendet werden.)
8. Geben Sie im Fenster zur Angabe des Datenbankadministrators einen Benutzernamen und ein Kennwort für den Datenbankadministrator ein. Bestätigen Sie das Kennwort, indem Sie dieses erneut eingeben, und klicken Sie anschließend auf **Weiter**. Der empfohlene Wert für beide Einträge lautet **db2admin**.
9. Das Programm beginnt mit der Installation der Datenbanksoftware. Die Ausführung dieses Prozesses kann einige Minuten dauern.
10. Klicken Sie im Fenster 'Setup abgeschlossen' auf **Beenden**, um die Installation abzuschließen.

Webserversoftware installieren

Tivoli PKI verwendet zur Unterstützung seiner Web-basierten Funktionen IBM WebSphere Application Server und IBM HTTP Server. Befolgen Sie beim Installieren der Software auf einer Windows NT-Plattform die angegebene Prozedur, um sicherzustellen, dass die Webserverprogramme für den Einsatz mit Tivoli PKI korrekt installiert sind. Sie müssen die Software auf der Maschine installieren, auf der auch die RA-Komponente installiert werden soll.

Zum Lieferumfang von Tivoli PKI gehört eine aktualisierte Version des WebSphere Application Server, die sich auf der CD von *Tivoli PKI für AIX und NT* befindet. Sie können die CD von WebSphere Application Server Version 2.02 zum Installieren des IBM HTTP Server und die Tivoli PKI-CD zum Installieren des WebSphere Application Server verwenden.

Obwohl WebSphere über eine Verwaltungsschnittstelle zum Verwalten von Servlets verfügt, ist es weder möglich noch erforderlich, Tivoli PKI-Servlets über diese Schnittstelle zu verwalten.

JDK installieren

Gehen Sie wie folgt vor, um JDK zu installieren:

1. Legen Sie die CD für WebSphere Application Server Version 2.0.2 in das CD-ROM-Laufwerk Ihres Systems ein.
2. Wechseln Sie in das Verzeichnis '\NT\jdk' und führen Sie das JDK-Programm 'setup.exe' aus.
3. Klicken Sie im Eingangsfenster auf **Weiter**.
4. Lesen Sie die Informationen im Fenster mit den Softwarelizenzvereinbarungen, und klicken Sie anschließend auf **Ja**, um diese zu akzeptieren.
5. Akzeptieren Sie im Fenster 'Komponenten wählen' die Standardauswahloptionen (Programmdateien, Bibliothek, Header-Dateien und Demo-Applets). Klicken Sie auf **Weiter**, um den Standardinstallationspfad zu verwenden. Wählen Sie andernfalls das gewünschte Laufwerk und den gewünschten Zielordner aus, in

dem JDK installiert werden soll, und klicken Sie anschließend auf **Weiter**. (Im vorliegenden Fall kann der Standardpfad verwendet werden.)

6. Überprüfen Sie im Fenster 'Kopiervorgang starten' die ausgewählten Optionen, und klicken Sie anschließend auf **Weiter**, um die Verarbeitung fortzusetzen.
7. Klicken Sie im Fenster für den Installationsabschluss auf die Option für **Beenden**.
8. Wenn die Readme-Datei angezeigt wird, lesen Sie die darin enthaltenen Informationen.

IBM HTTP Server installieren

Gehen Sie wie folgt vor, um IBM HTTP Server zu installieren:

1. Legen Sie die CD für WebSphere Application Server Version 2.0.2 in das CD-ROM-Laufwerk Ihres Systems ein.
2. Wechseln Sie in das Verzeichnis '\NT\httpd' und führen Sie das IHS-Programm 'setup.exe' aus.
3. Klicken Sie im Eingangsfenster auf **Weiter**.
4. Lesen Sie die Informationen im Fenster mit den Softwarelizenzvereinbarungen, und klicken Sie anschließend auf **Ja**, um diese zu akzeptieren.
5. Akzeptieren Sie im Fenster 'Zielpfad wählen' den Standardinstallationspfad, oder geben Sie den gewünschten Pfad an.
6. Klicken Sie auf **Weiter**.
7. Wählen Sie im Fenster 'Setup-Typ' die Option für **Angepasst** aus und klicken Sie anschließend auf **Weiter**.
8. Im Fenster 'Komponenten wählen' sind zwei Teilfenster enthalten. Auf der linken Seite werden die Namen der Komponentengruppen, auf der rechten Seite die Komponenten aufgelistet, aus denen diese Komponentengruppen bestehen. Wählen Sie links den Eintrag für **Basis** aus und nehmen Sie rechts die Auswahl für **Apache-Quelle** zurück.

Wenn Sie die **Dokumentation** nicht installieren wollen, nehmen Sie die Auswahl des entsprechenden Eintrags ebenfalls zurück. Klicken Sie auf **Weiter**, um die Verarbeitung fortzusetzen.

9. Klicken Sie im Menü 'Programmordner auswählen' auf **Weiter**, um den Standardprogrammordner zu akzeptieren. Geben Sie andernfalls den gewünschten Ordnernamen ein, und klicken Sie dann auf **Weiter**.
10. Geben Sie im Fenster mit den Informationen für den Dienst-Setup als **Benutzer-ID** den Wert `cfguser` sowie das Kennwort ein, das Sie für diesen Benutzereintrag erstellt haben, bestätigen Sie das Kennwort, und klicken Sie anschließend auf **Weiter**.
11. Im Fenster 'Setup abgeschlossen' können Sie nun auswählen, ob Sie das System sofort oder zu einem späteren Zeitpunkt erneut booten wollen. Wählen Sie die Option für ein späteres Booten (**Nein**) aus und klicken Sie anschließend auf **Beenden**.

Anmerkung: Nach der Installation des IBM HTTP Server müssen Sie für den Server-Dienst den manuellen Modus definieren, damit der Server nicht als Dienst gestartet wird. Gehen Sie hierzu wie folgt vor:

1. Wählen Sie **Start → Einstellungen → Systemsteuerung** aus.
2. Klicken Sie **Dienste** doppelt an und wählen Sie anschließend den Dienst **IBM HTTP Server** aus.
   a. Klicken Sie auf **Beenden** (wenn die Verarbeitung bereits gestartet wurde).
   b. Klicken Sie auf **Starten** und definieren Sie für die Option **Startart** die Einstellung **Manuell**.
   c. Klicken Sie auf **OK**.
   d. Klicken Sie auf **Schließen** und verlassen Sie die Systemsteuerung.

WebSphere Application Server installieren

Gehen Sie wie folgt vor, um WebSphere Application Server zu installieren:

1. Legen Sie die CD von *Tivoli Public Key Infrastructure für AIX und NT* in das CD-ROM-Laufwerk ein.
2. Wechseln Sie in das Verzeichnis '\WinNT\WebSphereAS-2031' und führen Sie das Programm 'was2031.exe' aus.
3. Klicken Sie im WebSphere Application Server-Fenster auf **Weiter**. Die Warnung zum Stoppen des IBM HTTP Server können Sie ignorieren.
4. Klicken Sie im Fenster für die Auswahl des Zielverzeichnisses auf **Weiter**, wenn Sie den Standardinstallationspfad verwenden wollen. Wählen Sie andernfalls das gewünschte Laufwerk und den gewünschten Zielordner aus, in dem die Software installiert werden soll, und klicken Sie anschließend auf **Weiter**.
5. Im Fenster für die Auswahl der Anwendungsserverkomponenten können Sie die Auswahl der **Dokumentation** und der **Beispiele** zurücknehmen. Alle anderen Komponenten sind jedoch erforderlich. Klicken Sie auf **Weiter**, um die Verarbeitung fortzusetzen.
6. Stellen Sie im Fenster für die Auswahl von JDK (Java Development Kit) oder der Laufzeitumgebung (Runtime Environment) sicher, dass **Java Development Kit 1.1.6** ausgewählt ist, und klicken Sie anschließend auf **Weiter**.
7. Wählen Sie im Fenster für die Auswahl der Anwendungsserver-Plug-ins **IBM HTTP Server Version 1.3.3.x** aus, und klicken Sie anschließend auf **Weiter**.
8. Klicken Sie im Fenster 'Programmordner auswählen' auf **Weiter**, um den Standardprogrammordner zu akzeptieren. Geben Sie andernfalls den gewünschten Ordnernamen ein, und klicken Sie dann auf **Weiter**.
9. Stellen Sie im Fenster für die Konfiguration des IBM HTTP Server sicher, dass der korrekte Pfad für die Adresse angezeigt

wird, unter der das Verzeichnis '\conf' des installierten IBM HTTP Server definiert ist, und klicken Sie anschließend auf **OK**.

10. Klicken Sie im Fenster für den Installationsabschluss auf die Option für **Beenden**.
11. Wenn die Readme-Datei angezeigt wird, lesen Sie die darin enthaltenen Informationen.
12. Im Fenster für den Neustart von Windows können Sie nun auswählen, ob Sie das System sofort oder zu einem späteren Zeitpunkt erneut booten wollen. Wählen Sie die Option für das sofortige Booten (**Ja**) aus, und klicken Sie anschließend auf **OK**.

IP-Aliasnamen definieren

Im Abschnitt „IP-Aliasnamen für den Webserver konfigurieren" auf Seite 44 finden Sie Informationen dazu, wie Tivoli PKI Ports auf dem Webserver konfiguriert, um gesicherte und nicht gesicherte Transaktionen zu verarbeiten. Wenn Sie mit einer anderen Konfiguration arbeiten wollen, müssen Sie zum Definieren dieser Ports IP-Aliasnamen verwenden.

IBM Directory installieren

Tivoli PKI verwendet das IBM Directory, um Informationen zu Zertifikaten, die von der Registrierungsfunktion ausgestellt wurden, zu speichern und zu verwalten. Verwenden Sie die in den folgenden Abschnitten beschriebenen Prozeduren, um die Directory-Software zu installieren und zu konfigurieren. Sie können diese Software auf einer fernen Maschine oder auf der Maschine installieren, auf der auch eine Tivoli PKI-Server-Komponente installiert werden soll.

Directory-Software installieren

Gehen Sie wie folgt vor, um die Directory-Software zu installieren:

1. Legen Sie die CD von IBM Directory Server in das CD-ROM-Laufwerk Ihres Systems ein, und führen Sie das Programm 'setup.exe' aus.

2. Wählen Sie im Fenster zur **Auswahl der Sprache für die Installation** die Installationssprache aus, und klicken Sie anschließend auf **Weiter**.
3. Klicken Sie im Eingangsfenster auf **Weiter**.
4. Wählen Sie im Fenster 'Komponenten wählen' die Option **SecureWay Directory und Client SDK installieren** aus, und klicken Sie anschließend auf **Weiter**.
5. Klicken Sie im Fenster 'Zielpfad wählen' auf **Weiter**, wenn Sie den Standardinstallationspfad verwenden wollen. Wählen Sie andernfalls einen anderen Zielpfad aus, und klicken Sie anschließend auf **Weiter**. Wenn Sie eine Nachricht erhalten, in der Sie darüber informiert werden, dass es sich bei der Installationspartition nicht um eine NTFS-Partition handelt, klicken Sie auf **OK**, um die Verarbeitung fortzusetzen.
6. Klicken Sie im Fenster 'Auswahl des Ordners' auf **Weiter**, um den Standardprogrammordner zu akzeptieren. Geben Sie andernfalls den gewünschten Ordnernamen ein, und klicken Sie dann auf **Weiter**.
7. Löschen Sie im Fenster 'Konfigurieren' die Auswahl aller Markierungsfelder, und klicken Sie anschließend auf **Weiter**.
8. Überprüfen Sie im Fenster 'Kopieren der Dateien für SecureWay Directory und Client SDK starten' die ausgewählten Optionen, und klicken Sie anschließend auf **Weiter**.
9. Klicken Sie auf **Ja**, um die Readme-Datei anzuzeigen, wenn Sie vom System dazu aufgefordert werden. Schließen Sie dann das Fenster.
10. Im Fenster 'Setup abgeschlossen' können Sie nun auswählen, ob Sie das System sofort oder zu einem späteren Zeitpunkt erneut booten wollen. Wählen Sie die Option für das sofortige Booten (**Ja**) aus, und klicken Sie anschließend auf **Beenden**.

Anmerkung: In einer Konfiguration mit mehreren Maschinen müssen Sie auf jedem Tivoli PKI-Server die Directory-Client-Software installieren, bevor Sie das Konfigurations-Applet für Tivoli PKI ausführen. Zum Instal-

lieren dieser Software müssen Sie die Directory-Client-Option von der Directory Server-CD auf allen Maschinen außer der Einheit installieren, auf der soeben die Directory-Server-Software installiert wurde. Die Namen der wichtigen Dateien, die auf allen Maschinen installiert werden müssen, lauten 'ldap.dll' und 'ldaploc1.dll'.

Directory unter Tivoli PKI verwenden

Vor der Installation oder Konfiguration der Tivoli PKI-Server-Komponenten müssen Sie verstehen, wie Tivoli PKI mit dem Directory zusammenarbeitet. Informationen zu den Directory-Schemavoraussetzungen und zur Konfiguration des Directories für den Einsatz unter Tivoli PKI finden Sie im Handbuch *Tivoli PKI Konfiguration.*

Systemeinstellungen bestätigen

Vor der Installation von Tivoli PKI sollten Sie mit der folgenden Prozedur sicherstellen, dass die u. a. Services sich im angezeigten Status befinden.

1. Melden Sie sich unter Windows NT als Konfigurationsbenutzer von Tivoli PKI an. (Diesem ist normalerweise der Benutzereintrag 'cfguser' zugeordnet.)
2. Wählen Sie **Start → Einstellungen → Systemsteuerung** aus.
3. Klicken Sie doppelt auf **Dienste** und bestätigen Sie die folgenden Statuswerte. Die beiden hervorgehoben dargestellten Dienstein-stellungen sind hierbei von besonderer Bedeutung:

DB2 - DB2	**Gestartet**	**Automatisch**
DB2 - DB2DAS00	Gestartet	Automatisch
DB2 Governor		Manuell
DB2 JDBC Applet Server		Manuell
DB2 Security Server		Manuell
IBM HTTP Server		**Manuell**
WebSphere Servlet Service		Manuell

4. Klicken Sie auf **Schließen** und verlassen Sie die Systemsteuerung.

Tivoli PKI installieren

Verwenden Sie die folgenden Richtlinien, um die Produktkomponenten von Tivoli PKI zu konfigurieren:

- Bitte beachten Sie, dass alle Serverprogramme auf derselben Plattform installiert werden müssen, im vorliegenden Fall also unter Windows NT.
- Wurde zuvor IBM KeyWorks Version 1.1.1 installiert, müssen Sie Tivoli PKI entweder auf einer anderen Maschine installieren oder die KeyWorks-Software und alle zugehörigen Anwendungen entfernen, bevor Sie das Installationsprogramm von Tivoli PKI starten.
- Wenn Sie Tivoli PKI in einer Konfiguration mit mehreren Maschinen installieren wollen, müssen Sie die Installationsprozeduren auf den gewünschten Maschinen wiederholen, bis alle Server-Komponenten installiert sind.
- Wenn Sie das RA Desktop-Applet installieren wollen, müssen Sie zuerst ein Installationsimage installieren. Anschließend muss das Image verteilt oder über das Netz zur Verfügung gestellt werden, damit die Benutzer das Installationsprogramm über eine lokale Windows-Maschine ausführen können. Instruktionen zum Installieren, Konfigurieren und Deinstallieren dieser Programme finden Sie in der Veröffentlichung *Tivoli PKI RA Desktop*.
- Wenn Sie das System nach der Installation der Softwarevoraussetzungen nicht erneut gestartet haben, müssen Sie jetzt einen Neustart durchführen. Stellen Sie sicher, dass die Umgebungsvariablen korrekt definiert sind, bevor Sie Tivoli PKI installieren.
- Verwenden Sie PING oder ein anderes Netzkonnektivitäts-Tool, um zu überprüfen, ob die Host-Namen und IP-Adressen gültig und auf dem DNS-Server Ihres Netzes definiert sind.

Serversoftware installieren

Gehen Sie wie folgt vor, um die Serversoftware zu installieren:

1. Melden Sie sich bei Windows NT mit dem Benutzernamen und dem Kennwort an, die Sie für diesen Zweck definiert haben (normalerweise 'cfguser'). Falls erforderlich, lesen Sie die Informationen im Abschnitt „Windows NT konfigurieren" auf Seite 96.
2. Beenden Sie alle aktiven Programme.
3. Legen Sie die CD von *Tivoli Public Key Infrastructure für AIX und NT* in ein lokal angeschlossenes CD-ROM-Laufwerk ein.
4. Wählen Sie **Start → Ausführen** aus und klicken Sie anschließend auf **Durchsuchen**, um zum CD-ROM-Laufwerk zu wechseln. Führen Sie dann die Datei 'setup.exe' aus. Beispiel:

   ```
   drive:\WinNT\TrustAuthority\setup
   ```

   Wenn Sie das Konfigurationsprogramm auf einer Maschine ausführen, die mit mehr als 256 MB Hauptspeicherplatz ausgerüstet ist, müssen Sie die Option '/z' hinzufügen, um die Speicherprüfung zu inaktivieren. Beispiel:

   ```
   drive:\WinNT\TrustAuthority\setup /z
   ```
5. Wählen Sie im Fenster für die Auswahl der Setup-Sprache eine Sprache für die aktuelle Installation aus, und klicken Sie dann auf **OK**. Der Standardwert ist **English**.
6. Lesen Sie die Informationen im Eingangsfenster und klicken Sie anschließend auf **Weiter**.
7. Wenn Sie anstelle der zum Lieferumfang von Tivoli PKI gehörenden Version eine eigenständige Version von IBM DB2 installiert haben, wird das Fenster 'Zielpfad wählen' aufgerufen. Klicken Sie auf **Weiter**, wenn Sie die Software im Standardpfad (c:\Program Files\IBM\Tivoli PKI) installieren wollen. Klicken Sie andernfalls auf **Durchsuchen**, um einen anderen Zielordner auszuwählen oder einzugeben, und klicken Sie anschließend auf **Weiter**.

8. Verwenden Sie im Fenster 'Komponenten wählen' die folgende Tabelle als Richtlinie. Markieren Sie die Komponenten, die Sie installieren möchten, nehmen Sie die Auswahl für die Komponenten zurück, die Sie nicht installieren möchten, und klicken Sie auf **Weiter**.

Komponente	Beschreibung
Tivoli PKI- und RA-Server	Installation der Tivoli PKI-Hauptprogramme und der RA-Server-Software, einschließlich aller Dateien, die für die Registrierungsfunktion erforderlich sind.
CA- und Prüf-Server	Installation der CA- und Prüfsubsystemprogramme.
Directory-Server	Installation der Software, die die Tivoli PKI-Komponenten benötigen, um mit dem Directory zu interagieren.
RA Desktop	Installation eines Installations-Images für das RA Desktop-Applet von Tivoli PKI.

Anmerkungen:

- Zu diesem Zeitpunkt stellt das Konfigurationsprogramm fest, ob die für die ausgewählten Komponenten erforderliche Software installiert ist und die korrekte Version aufweist. Wenn ein erforderliches Programm nicht verfügbar ist, wird das Konfigurationsprogramm beendet. Installieren Sie die erforderliche Software und starten Sie die Installationsprozedur erneut.
- Zur Vorbereitung der Datenbankkonfiguration überprüft das Konfigurationsprogramm auch den Benutzernamen, mit dem Sie sich angemeldet haben. Wenn der Benutzername länger als acht Zeichen ist, wird das Konfigurationsprogramm beendet. Melden Sie sich mit einem Benutzernamen an, der maximal acht Zeichen lang ist, und starten Sie die Installationsprozedur erneut.

- Wenn Sie die Option für **Tivoli PKI und RA-Server** auswählen und das Konfigurationsprogramm feststellt, dass mehr als eine Version von IBM WebSphere Application Server oder IBM HTTP Server vorhanden ist, werden Sie dazu aufgefordert, die gewünschte Version auszuwählen.

9. Klicken Sie im Fenster 'Programmordner auswählen' auf **Weiter**, wenn Sie ein Programmsymbol im Standardprogrammordner (Tivoli PKI) erstellen möchten. Geben Sie andernfalls den Namen des Ordners an, der verwendet werden soll, oder wählen Sie den Namen aus. Klicken Sie anschließend auf **Weiter**.
10. Klicken Sie im Fenster 'Setup abgeschlossen' auf **Beenden**, um den Installationsprozess zu starten. Das System kopiert die Dateien an die angeforderten Positionen und führt eine Reihe von Programmen aus, um die Installation von Tivoli PKI abzuschließen.
11. Führen Sie nach der Installation der Software einen Neustart des Systems durch.

Bootwerte ändern

Verwenden Sie diese Prozedur nur, wenn Sie einen der standardmäßigen Konfigurationswerte ändern wollen. Hierbei handelt es sich um die Werte, die bei der Ausführung des Konfigurations-Applets oder nach der Konfiguration des Systems nicht geändert werden können. Sie müssen alle Boot-Änderungen vornehmen, bevor Sie das Tivoli PKI-Konfigurationsprogramm für den Installationsabschluss ausführen. Tivoli PKI führt im Rahmen des Installationsabschlussprozesses ein Boot-Programm aus. Als Eingabe für dieses Boot-Programm wird ein SQL-Script mit dem Namen 'createconfig_start.sql' verwendet, das Standardwerte in die Konfigurationsdatenbank lädt und in der Datenbanktabelle 'ConfigDataTbl' Definitionen für Datenbanktabellen erstellt. Diese Tabelle enthält die Daten für die Systemkonfiguration aller Tivoli PKI-Komponenten. Verschiedene Werte in diesem SQL-Script können nach dem Starten des Konfigurationsprozesses nicht mehr geändert werden.

Anmerkung: In kritischen Situationen, in denen ein Standardwert zu Problemen in der Betriebsumgebung führen würde, können Sie vor der Konfiguration auch die Schablonendateien von Tivoli PKI ändern. Wenn Sie weitere Informationen hierzu benötigen, wenden Sie sich bitte an den zuständigen IBM Ansprechpartner.

Wenn Sie einen Boot-Wert ändern wollen, müssen Sie die Datei 'createconfig_start.sql' editieren. Diese Datei wird standardmäßig im Verzeichnis 'c:\Program Files\IBM\Trust Authority\bin' gespeichert.

Verwenden Sie die folgende Tabelle als Richtlinie für die Durchführung von Änderungen:

- Bei Windows NT können die Werte für DATABASE PATHNAME nicht geändert werden.
- Die registrierten Namen (DNs) für die Tivoli PKI-Registrierungsstelle, den Directory-Administrator und das Prüfsubsystem sind für den Benutzer transparent. Wenn Sie diese ändern wollen, müssen Sie darauf achten, dass nur das Attribut für den allgemeinen Namen (CN) geändert wird. Der DN-Basiswert für den Zertifikatsaussteller (CA), den Sie während der Konfiguration angegeben haben, wird auch für den von Ihnen ausgewählten allgemeinen Namen (CN) angewendet.

Feldname	Beschreibung	Standardwert
WS_RO_KEYSIZE	Schlüsselgröße für den Schlüsselring des Web-Servers. Die Optionen 0 - 3, die in der KeySize-Aufzählung definiert sind, sind wie folgt zugeordnet: ■ 0 = 512 ■ 1 = 768 ■ 2 = 1024 ■ 3 = 2048	0

Feldname	Beschreibung	Standardwert
APP_DN	Der registrierte Name (DN) der Registrierungsstelle (RA) von Tivoli PKI. Sie können lediglich den allgemeinen Namen (CN) ändern.	/C=US/O=Ihr Unternehmen/OU= Tivoli PKI/CN= Tivoli PKI RA
APP_CERT_LIFETIME	Die in Monaten angegebene Lebensdauer eines Nicht-CA-Zertifikats (z. B. eines Benutzer-, Server- oder RA-Zertifikats) im System. Der angegebene Wert muss auch in den Dateien 'jonahca.ini.tpl' und 'jonahra.ini.tpl' definiert werden.	36
APP_LDAP _DIRADMIN _DN	Der registrierte Name (DN) des Directory-Administrators. Sie können lediglich den allgemeinen Namen (CN) ändern.	/C=US/O=Ihr Unternehmen/OU =Tivoli PKI/CN= DirAdmin
APP_COMM_PORT	Der Kommunikations-Port, der zur Durchführung der Kommunikation zwischen dem Gerüst der Registrierungsfunktion und der Registrierungsstelle von Tivoli PKI verwendet wird.	29783

Feldname	Beschreibung	Standardwert
APP_SEC_MECH	Der Sicherheits-mechanismus der Anwendung. Standard-mäßig wird die RA-Datenbank-verschlüsselung inakti-viert. Wenn Sie den Wert auf 1 setzen, wird die Datenbank-verschlüsselung akti-viert.	0
CA_IBM_CA_CERT _LIFETIME	Die in Monaten ange-gebene Lebensdauer des CA-Zertifikats von Tivoli PKI.	36
CA_IBM_ADMIN_PORT	Der Verwaltungs-Port des Zertifikats-ausstellers (CA) von Tivoli PKI. Der ange-gebene Wert muss auch für den PORT-Eintrag in der Datei (irgAutoCA.ini.tpl) definiert werden, die im Verzeichnis 'cfg' gespeichert ist.	1835
ADT_DN	Der registrierte Name (DN) des Prüfsub-systems. Sie können lediglich den allgemei-nen Namen (CN) ändern.	/C=US/O=Ihr Unternehmen/OU =Tivoli PKI/CN =Tivoli PKI Audit

Konfigurationsprogramm für den Installationsabschluss ausführen

Nach der Installation der Tivoli PKI-Server-Software müssen Sie das Konfigurationsprogramm 'CfgPostInstall' für den Installationsabschluss ausführen. Sie müssen dieses Programm ausführen, bevor Sie Tivoli PKI mit dem Setup Wizard konfigurieren.

Von diesem Programm wird eine Web-Server-Konfigurationsdatei (httpd.conf) erstellt, die das Starten des Web-Servers mit den für Tivoli PKI erforderlichen Parametern ermöglicht. Es bereitet darüber hinaus den Web-Server für die Ausführung des Konfigurations-Applets vor, erstellt die Konfigurationsdatenbank und füllt die Datenbank mit den Standardkonfigurationsdaten.

Gehen Sie wie folgt vor, um das Konfigurationsprogramm für den Installationsabschluss auszuführen:

1. Melden Sie sich als Konfigurationsbenutzer von Tivoli PKI an. (Diesem ist der Benutzereintrag 'cfguser' zugeordnet.)
2. Prüfen Sie, ob auf dem Server ein Verzeichnis 'temp' vorhanden ist und ob es mit Hilfe der Umgebungsvariablen '%TEMP%' definiert wurde.
3. Wählen Sie **Start → Programme → Tivoli Public Key Infrastructure → Konfiguration zum Installationsabschluss** aus.
4. Geben Sie **exit** ein, um das Fenster zu schließen.

CfgPostInstall fordert Sie zum Prüfen des Kennworts für den Benutzereintrag 'cfguser' und anschließend zum Definieren und Bestätigen des Kennworts für das Steuerprogramm (CP) auf. Das Kennwort für 'cfguser' steuert den Zugriff auf den Benutzereintrag 'cfguser' und auf die CfgApplet-Wizard-Seite. Das Steuerprogrammkennwort schränkt den Zugriff auf das Steuerprogramm ein. Es wird empfohlen, für das Steuerprogramm und den Benutzereintrag 'cfguser' unterschiedliche Kennwörter zu definieren. Bei dem von Ihnen erstellten Kennwort für 'cfguser' muss es sich um ein gültiges Systemkennwort handeln, dessen Länge maximal acht Zeichen betragen darf.

Prüfliste für den Installationsabschluss

Verwenden Sie die folgenden Prüfliste, um sicherzustellen, dass alle Voraussetzungen erfüllt sind, um mit der Konfiguration von Tivoli PKI zu beginnen. Informationen zum Ausführen des Setup Wizard finden Sie im Handbuch *Tivoli PKI Konfiguration*:

1. Verwenden Sie die entsprechenden Windows NT-Tools, um eine Sicherungskopie des aktuellen Systems zu erstellen.
2. Erstellen Sie zur Unterstützung bei der späteren Fehlerbehebung eine Sicherungskopie der Windows-Registrierung, um sicherzustellen, dass eine Liste der gesamten installierten Software zur Verfügung steht.
3. Wenn Sie nicht beabsichtigen, die Standardkonfigurationswerte für Web-Server-Ports zu verwenden, müssen Sie die IP-Aliasnamen konfigurieren, bevor Sie den Setup Wizard ausführen. Die Konfigurationsprogramme verwenden diese Werte bei der Erstellung des CA-Zertifikats für Ihr System. Informationen dazu, wie Tivoli PKI Ports auf dem Web-Server konfiguriert und verwendet, um gesicherte und nicht gesicherte Transaktionen zu verarbeiten, finden Sie in „IP-Aliasnamen für den Webserver konfigurieren” auf Seite 44.
4. Entscheiden Sie, welche registrierten Namen (DNs) für den Tivoli PKI-CA und die zugehörigen Agenten, den Directory-Administrator und den Directory-Root verwendet werden sollen.

   Prüfen Sie die Richtlinien im Handbuch *Tivoli PKI Konfiguration*, um sicherzustellen, dass die registrierten Namen (DNs) für diese Objekte die gewünschte Zertifizierungshierarchie auch unterstützen.
5. Füllen Sie das *Tivoli PKI-Konfigurationsdatenformular* aus, das im Handbuch *Tivoli PKI Konfiguration* enthalten ist, um sich mit den Informationen vertraut zu machen, die Sie für die Konfiguration des Systems bereithalten müssen. Verwenden Sie dieses Formular, um Informationen zum jeweiligen System aufzuzeichnen, wie beispielsweise die Server-Host-Namen und die bevorzugten registrierten Namen (DN).

6. Zur Unterstützung der Konfiguration sollten Sie die folgenden Arbeitsschritte ausführen, um auf der Maschine, auf der der Setup Wizard ausgeführt werden soll, eine umfangreiche MS DOS-Umgebung mit Schiebeleisten zu definieren. In einer normalen Umgebung verfügt das DOS-Fenster nicht über Schiebeleisten und enthält nur 24 Zeilen an Daten.

   a. Melden Sie sich als Konfigurationsbenutzer von Tivoli PKI an. (Diesem ist normalerweise der Benutzereintrag 'cfguser' zugeordnet.)

   b. Wählen Sie **Start → Einstellungen → Systemsteuerung** aus.

   c. Klicken Sie doppelt auf der **Konsole** von MS DOS.

   d. Wählen Sie die Indexzunge **Layout** aus.

   e. Definieren Sie im Abschnitt **Fensterpuffergröße** für **Höhe** mindestens den Wert 1000 (der Maximalwert beträgt 9999) und klicken Sie dann auf **OK**.

Backup-Dienstprogramm ausführen

Das Backup-Dienstprogramm von Tivoli PKI (ta-backup) ist ein Tool zum Sichern von Konfigurationsdaten, die in keiner der DB2-Datenbanken gespeichert sind. Die zugehörigen Dateiinformationen wie z. B. Dateiberechtigungen etc. werden ebenfalls gesichert. Verwenden Sie zum Sichern von DB2-Datenbanken die entsprechenden DB2-Dienstprogramme.

Das Backup-Dienstprogramm akzeptiert einen Parameter, der das Verzeichnis angibt, in das Backup-Daten geschrieben werden sollen. Dieses Backup-Verzeichnis ist das Stammverzeichnis, das zum Speichern aller Datendateien eingesetzt wird. Um Namensunverträglichkeiten innerhalb des Backup-Verzeichnisses zu verhindern, speichert das Backup-Dienstprogramm Dateien mit derselben Verzeichnisstruktur, die auch auf dem gesicherten System definiert wurde.

Das folgende Beispiel illustriert die Programmsyntax:

```
ta-backup -d backup_directory
```

Hierbei steht `-d` *`backup_directory`* für das Verzeichnis, das für die Datensicherung verwendet werden soll. Der Standardpfad lautet '/usr/lpp/iau/backup'.

Gehen Sie wie folgt vor, um das Dienstprogramm 'ta-backup' im Offlinemodus auszuführen:

1. Melden Sie sich mit dem Benutzereintrag 'cfguser' an.
2. Erstellen Sie (optional) das Verzeichnis, in dem die Konfigurationsdaten von Tivoli PKI gesichert werden sollen. Beispiel:

   ```
   mkdir "c:\Program Files\IBM\Trust Authority\my_tabackup"
   ```

3. Wechseln Sie in das Verzeichnis 'bin' von Tivoli PKI. Der Standardpfad lautet 'c:\Program Files\IBM\Trust Authority\bin'.
4. Geben Sie den folgenden Befehl ein und definieren Sie den absoluten Pfad für das Verzeichnis, in dem die Daten gesichert werden sollen:

   ```
   ta-backup -d "c:\Program Files\IBM\Trust Authority\my_tabackup"
   ```

6

Tivoli PKI konfigurieren

Nach der Installation der Serversoftware von Tivoli Public Key Infrastructure (PKI) müssen Sie Konfigurationswerte angeben, um zu steuern, wie die Komponenten an Ihrem Standort konfiguriert werden. So müssen Sie beispielsweise die Position für die Serverprogramme definieren, registrierte Namen (DNs) angeben und die Registrierungsdomäne einrichten.

Während der Konfiguration sichert das System die angegebenen Werte in einer exportierbaren Datei. Diese Funktion ist nützlich, wenn mehrere Exemplare von Tivoli PKI konfiguriert werden sollen, die dieselbe Plattform verwenden und ähnlich konfiguriert sind. Wenn Sie ein neues Tivoli PKI-Exemplar installieren, können Sie die gesicherten Werte importieren und als Basis für die Konfiguration des neuen Systems verwenden.

Tivoli PKI enthält den Setup Wizard, ein Applet für die Angabe von Konfigurationsoptionen. Bevor Sie mit der Konfiguration des Tivoli PKI-Systems beginnen, sollten Sie sich mit dem Konfigurationsprozess vertraut machen und festlegen, wie das System in der verwendeten Umgebung eingerichtet werden soll. Stellen Sie die Informationen zu Ihrem System bereit, so dass sie bei der Ausführung des Setup Wizard schnell verfügbar sind. Darüber hinaus muss sichergestellt werden, dass das System korrekt konfiguriert ist, bevor Sie es einsetzen.

Das Handbuch *Tivoli PKI Konfiguration* enthält Informationen zur Konfigurationsvorbereitung, zur Angabe von Konfigurationsoptionen

sowie zur Vorbereitung des Systems für die Verwendung in einer Produktionsumgebung. Die folgenden Informationen sind beispielsweise in diesem Handbuch enthalten:

- Arbeitsblätter, die Sie beim Zusammenstellen von Informationen vor dem Starten des Setup Wizard unterstützen.
- Richtlinien für die Verwendung des DN-Editors zur Angabe eines gültigen registrierten Namens (DN).
- Empfehlungen für die Schritte, die ausgeführt werden sollten, bevor Tivoli PKI den beteiligten Benutzern zur Verfügung gestellt wird. Bitte beachten Sie, dass einige Schritte, wie beispielsweise das Ändern der Server-Kennwörter und das Sichern des soeben konfigurierten Systems, kritisch sind.
- Prozeduren für die Deinstallation der Software.

Das Handbuch *Konfiguration* ist für die Verwendung in einer Web-Umgebung konzipiert und bietet Folgendes:

- Taskorientierte Informationen wie z. B. Anweisungen zum Konfigurieren ferner Komponenten oder zur Prüfung der Konfiguration.
- Konzeptionelle Informationen wie z. B. eine Erläuterung zu Registrierungsdomänen oder eine Beschreibung zum Directory.
- Referenzinformationen wie z. B. ausführliche Beschreibungen zu den Werten, die bei der Verwendung des Setup Wizard angegeben werden können.

Für den Zugriff auf das Handbuch *Konfiguration* stehen folgende Möglichkeiten zur Verfügung:

- Klicken Sie nach dem Starten des Setup Wizard auf einen beliebigen Knopf **Hilfe** und anschließend auf das Buchsymbol, während Sie die Online-Hilfe anzeigen.
- Über die Website von Tivoli Public Key Infrastructure unter folgender Adresse:

  `http://www.tivoli.com/support`

7

Erste Schritte

Nach der Installation und Konfiguration des Tivoli PKI-Systems (PKI = Public Key Infrastructure) benötigen Sie Informationen zur Verwaltung des Systems sowie zur Verwendung der grafischen Benutzerschnittstellen, die vom System zur Verfügung gestellt werden. Die folgenden Abschnitte enthalten Verweise auf Dokumentationen, die Sie bei den ersten Schritten mit Tivoli PKI unterstützen. Lesen Sie die Informationen in diesen Dokumenten, um folgende Aufgaben auszuführen:

- Feinabstimmung des Systembetriebs, um beispielsweise das System für die Produktion zu sichern oder um fortlaufende Leistungsanpassungen vorzunehmen.
- Ausführen des RA Desktop für die Verwaltung von ausgestellten Zertifikaten und Zertifikatsanforderungen.
- Abrufen von Zertifikaten mit den Browserregistrierungsformularen der Registrierungsfunktion.
- Anpassen von Registrierungsprozessen, z. B. Ändern der HTML-Formulare für die Registrierung oder Unterstützung unterschiedlicher Zertifikatstypen.

Systemverwaltung

Tivoli Public Key Infrastructure stellt eine Reihe von Tools zur Verfügung, die Sie bei der Systemverwaltung unterstützen. Er umfasst folgendes:

- Ein Dienstprogramm zum Starten und Stoppen der Server-Komponenten in einem sicheren, durch Kennwörter geschützten Modus.
- Ein Dienstprogramm zur Definition von gesicherten Kennwörtern für die gesicherten Komponentenprogramme.
- Ein Dienstprogramm, mit dem Benutzern mit Verwaltungsaufgaben die Berechtigung zur Verwendung des RA Desktop erteilt werden kann.
- Ein Dienstprogramm, das dem Tivoli PKI-CA die gegenseitige Zertifizierung mit einem anderen CA bzw. das Einrichten einer CA-Hierarchie ermöglicht.
- Ein Dienstprogramm zur Integritätsprüfung für die Prüfdatenbank und für archivierte Prüfsätze.
- Ein Dienstprogramm für die Archivierung und Unterzeichnung der Prüfdatenbank.
- Ein Dienstprogramm, das zum Ausführen einer Rolloveroperation für den Root-CA-Schlüssel von einem nicht beschädigten Schlüsselpaar zum nächsten CA-Schlüsselpaar dient.
- Eine Gruppe von Dienstprogrammen, die zur Bereitstellung eines sicheren Verfahrens für authentifizierte Benutzer dient, mit dessen Hilfe diese mehrere digitale Zertifikate über einen einzigen Tivoli PKI-Aufruf anfordern können.

Das Handbuch *Tivoli PKI Systemverwaltung* enthält eine Beschreibung dieser Dienstprogramme und Richtlinien zur Durchführung von Verwaltungsaufgaben.So enthält das Handbuch beispielsweise Empfehlungen zur Verwaltung der Server-Komponenten und der zugehörigen Datenbanken.

Darüber hinaus werden die Schritte dokumentiert, die ausgeführt werden müssen, um die Systemkonfiguration abzuschließen und das System für die Verwendung in einer Produktionsumgebung zu sichern.

Das Handbuch *Systemverwaltung* ist für die Verwendung in einer Web-Umgebung konzipiert und bietet Folgendes:

- Taskorientierte Informationen wie z. B. Anweisungen zum Stoppen des Systems oder zum Archivieren der Prüfdatenbank.
- Konzeptionelle Informationen wie z. B. eine Erläuterung zur gegenseitigen Zertifizierung, eine Beschreibung des Tivoli PKI-CAs oder Einzelheiten zu Prüfereignissen.
- Referenzinformationen wie beispielsweise eine detaillierte Beschreibung der Konfigurationsdateiparameter.

Um auf das Handbuch *Systemverwaltung* zuzugreifen, müssen Sie die Website von Tivoli Public Key Infrastructure unter folgender Adresse aufrufen:

`http://www.tivoli.com/support`

RA-Verwaltung

Auf dem RA-Server werden Datensätze zu Registrierungsanforderungen und ausgestellten Zertifikaten in einer verschlüsselten Registrierungsdatenbank gespeichert. Die Auswertung von Registrierungsanforderungen und die Verwaltung von Datenbanksätzen sind Aufgaben, die von Programmen oder von Mitarbeitern mit Administratorberechtigung ausgeführt werden können.

Tivoli PKI stellt das RA Desktop-Applet zur Verfügung, das die Verarbeitung von Zertifikatsanforderungen und das Ausführen von Aktionen für ausgestellte Zertifikate durch berechtigte RA-Administratoren vereinfacht.

Der RA Desktop unterstützt die folgenden typischen Administratoraufgaben:

- Registrierungsanforderungen bearbeiten, deren Genehmigung ansteht.
- Den Gültigkeitszeitraum für Zertifikate ändern, deren Gültigkeit demnächst abläuft.
- Für Zertifikate feststellen, ob diese erneuert werden können.
- Zertifikate vorübergehend aussetzen.
- Zertifikate permanent widerrufen.

Im *Tivoli PKI Registration Authority Desktop* wird das RA Desktop-Applet beschrieben.

Das Handbuch *RA Desktop* ist für die Verwendung in einer Web-Umgebung konzipiert und bietet Folgendes:

- Taskorientierte Informationen wie z. B. Anweisungen zum Installieren von RA Desktop und zum Abrufen einer Gruppe von Zertifikaten, deren Gültigkeitszeitraum demnächst abläuft, oder zum Anzeigen des Protokolls der bisher für ein Zertifikat ausgeführten Aktionen.
- Konzeptionelle Informationen wie z. B. eine Erläuterung zu Registrierungsdomänen oder zur Gültigkeitsdauer eines Zertifikats.
- Referenzinformationen wie z. B. ausführliche Beschreibungen zu den Werten, die ein Registrator bei der Verwendung von RA Desktop angeben kann.

Für den Zugriff auf das *RA Desktop* stehen folgende Möglichkeiten zur Verfügung:

- Klicken Sie nach dem Starten des RA Desktop auf einen beliebigen Knopf **Hilfe** und anschließend auf das Buchsymbol, während Sie die Online-Hilfe anzeigen.
- Über die Website von Tivoli Public Key Infrastructure unter folgender Adresse:

  `http://www.tivoli.com/support`

Registrierung und Zertifizierung

Verwenden Sie die mit der Registrierungsanwendung zur Verfügung stehenden Browser-Registrierungsformulare, um auf einfache Weise eine Registrierung für Browser-, Server- und Einheitenzertifikate durchzuführen. Wenn Ihre Anforderung genehmigt wird, wird das Zertifikat automatisch heruntergeladen. Darüber hinaus können Sie die Browser-Formulare verwenden, um eine Vorabregistrierung für Zertifikate durchzuführen, die mit einer PKIX-Anwendung verwendet werden können. Wenn die Vorabregistrierungsanforderung genehmigt wird, erhalten Sie Informationen, mit denen Sie das Zertifikat zu einem geeigneten Zeitpunkt abrufen können.

Das *Tivoli PKI Benutzerhandbuch* enthält eine Beschreibung der Browserregistrierungsformulare und enthält Folgendes:

- Taskorientierte Informationen wie z. B. Anweisungen zum Registrieren für ein Browserzertifikat oder zum Verlängern von Zertifikaten, deren Gültigkeitszeitraum demnächst abläuft.
- Konzeptionelle Informationen wie z. B. eine Erläuterung zur Vorabregistrierung oder zu Serverzertifikaten.

Um auf das *Benutzerhandbuch* zuzugreifen, müssen Sie die Website von Tivoli Public Key Infrastructure unter folgender Adresse aufrufen:

`http://www.tivoli.com/support`

Anpassung

Tivoli PKI bietet Ihnen flexible Möglichkeiten zum Implementieren von Registrierungsprozessen in Ihrem Unternehmen. Sie können mit diesem Produkt z. B. die folgenden Aktivitäten steuern:

- Die Darstellung der Browserregistrierungsformulare sowie die hierbei verwendete Sprache
- Zertifizierungsregeln
- Inhalt von Benachrichtigungsbriefen, die an Benutzer gesendet werden, die sich für Zertifikate registrieren lassen
- Regel-Exits zur Steuerung verschiedener automatischer Verarbeitungsoperationen

Das Handbuch *Tivoli PKI Anpassung* enthält eine Beschreibung der verschiedenen Möglichkeiten, die bei der Anpassung der Registrierungsfunktion zur Verfügung stehen und umfasst Folgendes:

- Taskorientierte Informationen wie z. B. Anweisungen zum Hinzufügen eines Registrierungsfeldes oder zum Ändern eines Zertifikatsprofils.
- Konzeptionelle Informationen wie z. B. eine Erläuterung zur Vorabregistrierung, zu Unternehmensregeln oder zur Zugriffssteuerung.
- Referenzinformationen, wie beispielsweise eine detaillierte Beschreibung der Zertifikatstypen und der Konfigurationsdatei der Registrierungsfunktion.

Um auf das Handbuch *Anpassung* zuzugreifen, müssen Sie die Website von Tivoli Public Key Infrastructure unter folgender Adresse aufrufen:

`http://www.tivoli.com/support`

Glossar

In diesem Glossar werden alle Termini und Abkürzungen definiert, die in diesem Handbuch verwendet werden und die möglicherweise neu oder unbekannt und von Bedeutung sind.

A

Abstract Syntax Notation One (ASN.1)
Eine ITU-Notation, die zum Definieren der Syntax von Informationsdaten benutzt wird. Sie definiert eine Reihe einfacher Datentypen und gibt eine Notation für die Identifizierung dieser Typen und die Angabe von Werten für diese Typen an. Diese Notationen können verwendet werden, wenn es erforderlich ist, die abstrakte Syntax von Informationen zu definieren, ohne damit die Art der Verschlüsselung dieser Informationen für die Übertragung zu beeinträchtigen.

ACL
Access Control List - Zugriffssteuerungsliste.

Aktionsprotokoll
Die Aufzeichnung aller Ereignisse, die während der gesamten Gültigkeitsdauer eines Identitätsnachweises aufgetreten sind.

American National Standard Code for Information Interchange (ASCII)
Der Standardcode, der für den Austausch von Informationen zwischen Datenverarbeitungssystemen, DFV-Systemen und zugehöriger Hardware verwendet wird. ASCII verwendet einen codierten Zeichensatz, der aus Zeichen von 7 Bit Länge (bzw. 8 Bit bei Paritätsprüfung) besteht. Der Zeichensatz besteht hierbei aus Steuerzeichen und Schriftzeichen.

American National Standards Institute (ANSI)
Eine Organisation, die die Verfahrensweisen definiert, mit deren Hilfe akkreditierte Organisationen freiwillig eingehaltene Industriestandards in den Vereinigten Staaten festlegen und verwalten. Ihr gehören Hersteller, Verbraucher und allgemeine Interessenvertretungen an.

Anforderungs-ID
Ein aus 24 bis 32 Zeichen bestehender ASCII-Wert, der zur eindeutigen Identifikation einer Zertifikatsanforderung gegenüber der RA dient. Dieser Wert kann bei der Transaktion für die Zertifikatsanforderung verwendet werden, um den Status der Anforderung oder des zugehörigen Zertifikats abzurufen.

ANSI
American National Standards Institute.

Applet
Ein in der Programmiersprache Java geschriebenes Computerprogramm, das innerhalb eines Java-kompatiblen Webbrowsers ausgeführt werden kann. Wird auch als Java-Applet bezeichnet.

Art
Siehe Objektart.

ASCII
American National Standard Code for Information Interchange.

ASN.1
Abstract Syntax Notation One.

Asymmetrische Verschlüsselung
Ein Verschlüsselungsverfahren, das zur Ver- und Entschlüsselung unterschiedliche, asymmetrische Schlüssel verwendet. Jedem Benutzer wird hierbei ein Schlüsselpaar zugeordnet, das einen allgemeinen, für alle zugänglichen Schlüssel und einen privaten Schlüssel umfasst, der nur dem jeweiligen Benutzer bekannt ist. Eine gesicherte Transaktion kann ausgeführt werden, wenn der öffentliche Schlüssel sowie der zugehörige private Schlüssel übereinstimmen. In diesem Fall kann die Transaktion entschlüsselt werden. Dieses Verfahren wird auch als Verschlüsselung auf der Basis von Schlüsselpaaren bezeichnet. *Gegensatz zu* Symmetrische Verschlüsselung.

Asynchrone Übertragung
Ein Übertragungsmodus, bei dem Sender und Empfänger nicht gleichzeitig vorhanden sein müssen.

Authentifizierung
Der Vorgang, bei dem die Identität eines Teilnehmers an einer Übertragung zuverlässig überprüft wird.

B

Base64-Verschlüsselung
Ein häufig verwendetes Verfahren bei der Übertragung von Binärdaten mit MIME.

Basic Encoding Rules (BER)
Die Regeln, die in ISO 8825 für die Verschlüsselung von in ASN.1 beschriebenen Dateneinheiten angegeben sind. Die Regeln geben das Verschlüsselungsverfahren, jedoch nicht die abstrakte Syntax an.

Benutzerauthentifizierung
Der Prozess, mit dem überprüft wird, ob der Absender einer Nachricht die berechtigte Person ist, als die er sich ausgibt. Der Prozess überprüft außerdem, ob ein Kommunikationsteilnehmer auch tatsächlich mit dem erwarteten Endbenutzer oder System in Verbindung steht.

BER

Basic Encoding Rules.

Berechtigung

Die Erlaubnis, auf eine Ressource zuzugreifen.

Bestreiten

Etwas als unwahr zurückweisen. Dies ist z. B. dann der Fall, wenn ein Benutzer abstreitet, eine bestimmte Nachricht gesendet oder eine bestimmte Anforderung übergeben zu haben.

Browser

Siehe Web-Browser.

Browser-Zertifikat

Ein digitales Zertifikat, das auch als Zertifikat der Client-Seite bezeichnet wird. Es wird von einem CA über einen für SSL aktivierten Web-Server ausgestellt. Die Schlüssel in einer verschlüsselten Datei ermöglichen dem Inhaber des Zertifikats das Verschlüsseln, Entschlüsseln und Unterzeichnen von Daten. Normalerweise werden diese Schlüssel im Web-Browser gespeichert. In bestimmten Anwendungen können die Schlüssel auf Smart-Cards oder anderen Speichermedien gespeichert werden. *Siehe auch* Digitales Zertifikat.

Bytecode

Maschinenunabhängiger Code, der mit dem Java-Compiler generiert und mit dem Java-Interpreter ausgeführt wird.

C

CA

Certificate Authority - Zertifikatsaussteller.

CA-Hierarchie

Bei Tivoli PKI eine Sicherungsstruktur, bei der ein CA auf der höchsten Ebene positioniert ist. Anschließend können bis zu vier weitere Ebenen mit untergeordneten CAs definiert werden. Wenn Benutzer oder Server bei einem Zertifikatsaussteller registriert werden, wird ihnen ein von diesem Aussteller unterzeichnetes Zertifikat zugeordnet. Außerdem übernehmen sie die Zertifizierungshierarchie der übergeordneten Ebenen.

CA-Server

Der Server für die CA-Komponente von Tivoli PKI.

CAST-64

Ein Block-Cipher-Algorithmus, der mit einer Blockgröße von 64 Bit und einem 6-Bit-Schlüssel arbeitet. Er wurde von Carlisle Adams und Stafford Tavares entwickelt.

CA-Zertifikat
Ein Zertifikat, das vom Web-Browser eines Benutzers auf dessen Anforderung hin von einem nicht identifizierten CA akzeptiert wird. Der Browser kann dann dieses Zertifikat verwenden, um für die Kommunikation mit Servern, die über Zertifikate dieses CAs verfügen, eine Authentifizierung durchzuführen.

CCA
IBM Common Cryptographic Architecture.

CDSA
Common Data Security Architecture.

CGI
Common Gateway Interface.

Client
(1) Eine Funktionseinheit, die gemeinsam benutzte Services von einem Server empfängt. (2) Ein Computer oder Programm, der/das Services von einem anderen Computer oder Programm anfordert.

Client/Server
Ein Modell für die verteilte Verarbeitung, bei dem ein Programm an einem Standort eine Anforderung an ein Programm an einem anderen Standort sendet und auf eine Antwort wartet. Das anfordernde Programm wird als Client, das antwortende als Server bezeichnet.

Codeunterzeichnung
Ein Verfahren zum Unterzeichnen ausführbarer Programme mit einer digitalen Unterschrift. Die Codeunterzeichnung dient zur Verbesserung der Zuverlässigkeit von Softwarekomponenten, die über das Internet verteilt werden.

Common Cryptographic Architecture (CCA)
IBM Software, die einen konsistenten Verschlüsselungsansatz auf den wichtigsten IBM Computerplattformen bietet. Sie unterstützt Anwendungssoftware, die in einer Vielzahl von Programmiersprachen geschrieben wurde. Die Anwendungssoftware kann hierbei die CCA-Services aufrufen, um eine breite Palette kryptografischer Funktionen (einschließlich der DES- und der RSA-Verschlüsselung) auszuführen.

Common Data Security Architecture (CDSA)
Eine Initiative zum Definieren eines umfassenden Ansatzes für Sicherheitsservices und Sicherheitsverwaltungsoperationen bei computerbasierten Sicherheitsanwendungen. Diese Architektur wurde von Intel entworfen und dient dazu, Computerplattformen für Anwendungen sicherer zu gestalten.

Common Gateway Interface (CGI)
Ein Standardverfahren zum Übertragen von Informationen zwischen Web-Seiten und Webservern.

CRL

Certificate Revocation List - Zertifikatswiderrufsliste.

CRL-Publikationsintervall

Dieses Intervall wird in der CA-Konfigurationsdatei definiert und gibt das Zeitintervall zwischen zwei Publikationen der Zertifikatswiderrufsliste im Directory an.

D

Dämon

Ein Programm, das Tasks im Hintergrund ausführt. Es wird implizit aufgerufen, wenn eine Bedingung auftritt, die die Hilfe des Dämons erforderlich macht. Es ist nicht erforderlich, dass der Benutzer über die Ausführung des Dämons unterrichtet wird, da der Dämon normalerweise vom System automatisch gestartet wird. Ein Dämon kann über eine unbegrenzte Zeit hinweg ausgeführt oder vom System in bestimmten Zeitintervallen erneut generiert werden.
Der Terminus (englisch *demon*) stammt aus der Mythologie. Später wurde er aber als Akronym für den Ausdruck ″Disk And Execution MONitor″ (Platten- und Ausführungsüberwachungsprogramm) erklärt.

Data Encryption Standard (DES)

Eine Verschlüsselungs-Block-Cipher, die 1977 von der US-Regierung als offizieller Standard definiert und übernommen wurde. Dieser Standard wurde ursprünglich von IBM entwickelt. DES wurde seit seiner Veröffentlichung umfassend untersucht und stellt ein allgemein bekanntes und häufig verwendetes Verschlüsselungssystem zur Verfügung.
Bei DES handelt es sich um ein symmetrisches Verschlüsselungssystem. Um es für die Datenübertragung einzusetzen, müssen sowohl der Sender als auch der Empfänger den selben, geheimen Schlüssel kennen. Dieser Schlüssel wird zum Ver- und Entschlüsseln der Nachricht verwendet. DES kann außerdem zur Durchführung von Verschlüsselungsoperationen für einzelne Benutzer eingesetzt werden, z. B. zum Speichern von verschlüsselten Dateien auf einer Festplatte. DES arbeitet mit einer Blockgröße von 64 Bit und verwendet für die Verschlüsselung einen 56-Bit-Schlüssel. Ursprünglich wurde dieser Standard für die Hardwareimplementierung entwickelt. DES wird von NIST alle fünf Jahre erneut als offizieller Verschlüsselungsstandard der US-Regierung zertifiziert.

Datenspeicherbibliothek (DL)

Ein Modul, das den Zugriff auf permanente Datenspeicher mit Zertifikaten, CRLs, Schlüsseln, Regeln und anderen sicherheitsrelevanten Objekten ermöglicht.

DEK

Document Encryption Key = Dokumentverschlüsselungsschlüssel.

DER

Distinguished Encoding Rules.

DES

Data Encryption Standard.

Diffie-Hellman

Ein Verfahren zur Datenverschlüsselung, das auf der Verwendung eines gemeinsamen Schlüssels auf einem nicht gesicherten Medium basiert und nach seinen Erfindern (Whitfield Diffie und Martin Hellman) benannt wurde.

Digitales Zertifikat

Ein elektronischer Identitätsnachweis, der von einer zuverlässigen Stelle für eine Person oder Entität ausgestellt wird. Jedes Zertifikat ist mit dem privaten Schlüssel des CAs unterzeichnet. Es bürgt für die Identität einer Person, eines Unternehmens oder einer Organisation.

Abhängig vom Aufgabenbereich des CAs kann das Zertifikat die Berechtigung seines Inhabers bestätigen, e-Business-Transaktionen über das Internet auszuführen. In gewisser Weise hat ein digitales Zertifikat eine ähnliche Funktion wie ein Führerschein oder ein Meisterbrief. Es bestätigt, dass der Inhaber des entsprechenden privaten Schlüssels berechtigt ist, bestimmte e-Business-Aktivitäten auszuführen.

Ein Zertifikat enthält Informationen über die Entität, die von ihm zertifiziert wird, gibt an, ob es sich um eine Person, eine Maschine oder ein Computerprogramm handelt und enthält als Teil dieser Informationen den zertifizierten öffentlichen Schlüssel dieser Entität.

Digitale Unterschrift

Eine codierte Nachricht, die an Dokumente oder Daten angefügt wird, und die Identität des Absenders nachweist.

Eine digitale Unterschrift gewährleistet ein höheres Maß an Sicherheit als eine physische Unterschrift, da es sich hierbei nicht lediglich um einen verschlüsselten Namen oder eine Reihe einfacher Identifikationscodes handelt. Eine digitale Unterschrift enthält eine verschlüsselte Zusammenfassung der unterzeichneten Nachricht. Durch das Anfügen einer digitalen Unterschrift an eine Nachricht lässt sich der Absender also zweifelsfrei feststellen. (Die Unterschrift kann nur mit Hilfe des Schlüssels des Absenders erstellt werden.) Außerdem ermöglicht sie die Absicherung des Inhalts der unterzeichneten Nachricht, da die verschlüsselte Nachrichtenzusammenfassung mit dem Nachrichteninhalt übereinstimmen muss. Andernfalls wird die Unterschrift nicht als gültig identifiziert. Eine digitale Unterschrift kann also nicht von einer Nachricht kopiert und für eine andere Nachricht verwendet werden, da sonst die Zusammenfassung (Hash-Code) nicht übereinstimmen würde. Alle Änderungen an der unterzeichneten Nachricht führen automatisch zum Verlust der Gültigkeit der Unterschrift.

Digitale Zertifizierung

Siehe Zertifizierung.

Digital Signature Algorithm (DSA)

Ein auf öffentlichen Schlüsseln basierender Algorithmus, der zum Standard für digitale Unterschriften (Digital Signature Standard = DSS) gehört. Er kann nur für digitale Unterschriften, jedoch nicht für die Verschlüsselung verwendet werden.

Directory

Eine hierarchische Struktur, die als globales Repository für Informationen zur Datenkommunikation (wie beispielsweise E-Mail oder Austausch von verschlüsselten Daten) konzipiert ist. Im Directory werden bestimmte Elemente gespeichert, die für die PKI-Struktur (PKI = Public Key Infrastructure) unbedingt erforderlich sind. Hierzu gehören die folgenden Elemente: öffentliche Schlüssel, Zertifikate und Zertifikatswiderrufslisten (CRLs).

Die Daten im Directory sind hierarchisch in einer Baumstruktur organisiert, wobei die oberste Ebene der Baumstruktur das Root-Verzeichnis ist. Häufig stehen Organisationen einer höheren Ebene für einzelne Länder, Regierungen oder Unternehmen. Benutzer oder Einheiten werden im Allgemeinen als ″Blätter″ einer solchen Baumstruktur dargestellt. Diese Benutzer, Organisationen, Standorte, Länder und Einheiten haben jeweils ihren eigenen Eintrag. Jeder Eintrag besteht aus Attributen, denen verschiedene Typen zugewiesen sind. Diese enthalten Informationen zu den Objekten, für die der jeweilige Eintrag steht.

Jeder Eintrag im Directory ist mit einem zugeordneten registrierten Namen (DN = Distinguished Name) verbunden. Dieser ist eindeutig, wenn der Eintrag ein Attribut umfasst, das für das tatsächliche Objekt als eindeutig bekannt ist. Im folgenden DN-Beispiel wurde als Land (C = Country) US, als Unternehmen (O = Organization) IBM, als Unternehmenseinheit (OU = Organization Unit) Trust und als allgemeiner Name (CN = Common Name) der Wert CA1 angegeben.

```
C=US/O=IBM/OU=Trust/CN=CA1
```

Directory-Server

In Tivoli PKI das IBM Directory. Dieses Directory unterstützt die LDAP-Standards und verwendet DB2 als Basissystem.

Distinguished Encoding Rules (DER)

Durch DER werden bestimmte Einschränkungen für BER definiert. Mit DER kann genau ein bestimmter Verschlüsselungstyp aus den verfügbaren und auf der Basis der Verschlüsselungsregeln als zulässig definierten Typen ausgewählt werden. Hierdurch werden alle Senderoptionen eliminiert.

DL

Data Storage Library = Datenspeicherbibliothek.

DN

Distinguished Name - Registrierter Name.

Dokumentverschlüsselungsschlüssel (DEK)

Normalerweise ein symmetrischer Ver-/Entschlüsselungsschlüssel, z. B. DES.

Domäne
Siehe Sicherheitsdomäne *und* Registrierungsdomäne.

DSA
Digital Signature Algorithm.

E

e-Business
Das Durchführen geschäftlicher Transaktionen über Netze und Computer, z. B. der Kauf und Verkauf von Waren und Dienstleistungen sowie der Transfer von Zahlungsmitteln mit Hilfe der digitalen Kommunikation.

e-Commerce
Unternehmensübergreifende Transaktionen wie beispielsweise der Kauf und Verkauf von Waren und Dienstleistungen (zwischen Unternehmen und ihren Kunden, Lieferanten, Subunternehmen und anderen) über das Internet. E-Commerce stellt einen Kernbestandteil des e-Business dar.

Endentität
Der Gegenstand eines Zertifikats, bei dem es sich nicht um einen CA handelt.

Entschlüsseln
Den Verschlüsselungsprozess rückgängig machen.

Exemplar
Bei DB2 bezeichnet man als Exemplar eine logische Datenbankverwaltungsumgebung zum Speichern von Daten und Ausführen von Anwendungen. Es ermöglicht die Definition einer allgemeinen Gruppe von Konfigurationsparametern für verschiedene Datenbanken.

Extranet
Ein Netz, das auf dem Internet basiert und eine ähnliche Technologie einsetzt. Unternehmen beginnen momentan mit dem Einsatz des Web Publishings, elektronischen Handels und der Nachrichtenübertragung sowie der Verwendung von Groupware für verschiedene Gruppen von Kunden, Partnern und internen Mitarbeitern.

F

File Transfer Protocol (FTP)
Ein Client/Server-Protokoll im Internet, das zum Übertragen von Dateien zwischen Computern benutzt wird.

Firewall
Ein Gateway zwischen Netzen, der den Informationsfluss zwischen diesen einschränkt. Normalerweise dienen Firewalls dem Schutz interner Netze gegen die nicht berechtigte Verwendung durch externe Personen.

FTP
File Transfer Protocol.

G

Gateway
Eine Funktionseinheit, mit deren Hilfe nicht kompatible Netze oder Anwendungen Daten austauschen können.

Gegenseitige Zertifizierung
Ein Trust-Modell, bei dem ein CA für einen anderen CA ein Zertifikat ausstellt, das den öffentlichen Schlüssel enthält, der dem entsprechenden privaten Unterschriftsschlüssel zugeordnet ist. Ein gegenseitig zertifiziertes Zertifikat ermöglicht Client-Systemen oder Endentitäten in einer Verwaltungsdomäne die sichere Kommunikation mit Client-Systemen oder Endentitäten in einer anderen Domäne.

Gesicherte Computerbasis (TCB)
Die Software- und Hardwareelemente, die zur Umsetzung der Computersicherheitsregeln eines Unternehmens verwendet werden. Alle Elemente oder Teilelemente, die zur Implementierung der Sicherheitsregeln eingesetzt werden können, sind sicherheitsrelevant und Bestandteil der TCB. Bei der TCB handelt es sich um ein Objekt, das durch die Sicherheitsperipherie begrenzt wird. Die Mechanismen, die zur praktischen Umsetzung der Sicherheitsregeln eingesetzt werden, dürfen nicht umgangen werden können und müssen verhindern, dass Programme Zugriff auf Systemprivilegien erlangen können, für die sie nicht berechtigt sind.

H

Hierarchie
Die Organisation von Zertifikatsausstellern (CAs) innerhalb einer Trust-Kette. Diese beginnt mit einem selbst unterzeichnenden CA oder übergeordneten Root-CA, der sich an der höchsten Position befindet, und endet mit dem CA, der Zertifikate für Endbenutzer ausstellt.

Höchster CA
Der CA, der innerhalb der PKI-CA-Hierarchie die höchste Position einnimmt.

HTML
Hypertext Markup Language.

HTTP
Hypertext Transaction Protocol.

HTTP-Server
Ein Server, der die Web-gestützte Kommunikation mit Browsern und anderen Programmen im Netz steuert.

Hypertext
Textsegmente, die einzelne oder mehrere Wörter umfassen oder Bilder enthalten, auf die der Leser mit der Maus klicken kann, um ein anderes Dokument aufzurufen und anzuzeigen. Diese Textsegmente werden als Hyperlinks bezeichnet. Ruft der Leser diese anderen Dokumente auf, stellt er zu diesen eine Hyperlink-Verbindung her.

Hypertext Markup Language (HTML)
Eine Formatierungssprache für das Codieren von Web-Seiten. HTML basiert auf SGML (Standard Generalized Markup Language).

Hypertext Transaction Protocol (HTTP)
Ein Client/Server-Protokoll für das Internet, mit dem Hypertext-Dateien im Web übertragen werden.

I

ICL
Issued Certificate List - Liste der ausgestellten Zertifikate.

Identitätsnachweis
Vertrauliche Informationen, die verwendet werden, um beim Austausch von Daten während der Authentifizierung die eigene Identität zu belegen. In Network Computing-Umgebungen ist die am häufigsten verwendete Form des Identitätsnachweises ein Zertifikat, das von einem CA erstellt und unterzeichnet wurde.

IniEditor
Bei Tivoli PKI ein Tool, mit dem Konfigurationsdateien editiert werden können.

Integrität
Ein System schützt seine Datenintegrität, wenn es die Änderung dieser Daten durch nicht berechtigte Personen verhindert. (Im Gegensatz hierzu versteht man unter dem Schutz der Vertraulichkeit von Daten, wenn verhindert wird, dass diese unberechtigten Personen zugänglich gemacht werden.)

Integritätsprüfung
Die Prüfung der Protokolleinträge, die für Transaktionen mit externen Komponenten aufgezeichnet wurden.

International Standards Organization (ISO)
Eine internationale Organisation, die sich mit der Entwicklung und Veröffentlichung von Standards befasst.

International Telecommunication Union (ITU)
Eine internationale Organisation, in der Verwaltungs- und private Industriebereiche globale Datenfernübertragungsnetze und -services koordinieren. Bei der Veröffentlichung von Informationen zur Datenfernübertragungstechnologie sowie den entsprechenden Regelwerken und Standards nimmt sie eine führende Position ein.

Interne Struktur
Siehe Schema.

Internet
Ein weltweiter Verbund von Netzen, die die elektronische Verbindung zwischen Computern und die Kommunikation zwischen den Computern über Softwareeinrichtungen wie elektronische Post (E-Mail) oder Web-Browser ermöglichen. So sind beispielsweise die meisten Universitäten in ein Netz eingebunden, das seinerseits eine Verbindung zu anderen ähnlichen Netzen hat, die zusammen das Internet bilden.

Internet Engineering Task Force (IETF)
Eine Gruppe, die sich schwerpunktmäßig mit dem Entwickeln und Definieren von Protokollen für das Internet befasst. Sie repräsentiert eine internationale Gruppe von Netzdesignern, -bedienern, -herstellern und -forschern. Die Aufgabe der IETF ist die Entwicklung der Internet-Architektur sowie die Gewährleistung der reibungslosen Verwendung des Internets.

Intranet
Ein Netz innerhalb eines Unternehmens, das sich im Allgemeinen hinter Firewalls befindet. Es basiert auf dem Internet und setzt eine ähnliche Technologie ein. Vom technischen Standpunkt aus ist ein Intranet eine Erweiterung des Internets. Zu den in beiden Netzen benutzten Komponenten gehören z. B. HTML und HTTP.

IPSec
Ein von der IETF entwickelter IPS-Standard (IPS = Internet Protocol Security). IPSec ist ein Protokoll der Vermittlungsschicht, das entwickelt wurde, um Services für die Gewährleistung der Sicherheit bei der Verschlüsselung zur Verfügung zu stellen, die kombinierte Funktionen zur Authentifizierung, Sicherung der Integrität, Zugriffssteuerung und Wahrung der Vertraulichkeit flexibel unterstützen. Aufgrund seiner leistungsfähigen Funktionen bei der Authentifizierung wurde dieser Standard von vielen Lieferanten von VPN-Produkten als Protokoll zum Aufbau sicherer Punkt-zu-Punkt-Verbindungen im Internet übernommen.

ISO
International Standards Organization.

ITU
International Telecommunication Union.

J

Java
Von Sun Microsystems, Incorporated, entwickelte plattformunabhängige Computertechnologien, die für den Netzbetrieb optimiert sind. Die Java-Umgebung besteht aus dem Java-Betriebssystem (Java-OS), den virtuellen Maschinen für verschiedene Plattformen, der objektorientierten Java-Programmiersprache und einer Reihe von Klassenbibliotheken.

Java-Anwendung
Ein eigenständiges Programm, das in der Programmiersprache Java geschrieben ist. Es wird außerhalb eines Web-Browsers ausgeführt.

Java-Applet
Siehe Applet. *Gegensatz zu* Java-Anwendung.

Java-Klasse
Eine Einheit mit Java-Programmcode.

Java-Sprache
Eine von Sun Microsystems entwickelte Programmiersprache, die speziell für die Verwendung in Applet- und Agent-Anwendungen konzipiert wurde.

Java Virtual Machine (JVM)
Der Teil der Java-Laufzeitumgebung, der zum Interpretieren von Bytecodes eingesetzt wird.

K

KeyStore (Schlüsselspeicher)
Eine DL zum Speichern von Identitätsnachweisen für Tivoli PKI-Komponenten, z. B. Schlüssel und Zertifikate, in einem verschlüsselten Format.

Klartext
Nicht verschlüsselte Daten. *Synonym zu* unverschlüsselter Text.

Klasse
Beim objektorientierten Entwurf bzw. bei der objektorientierten Programmierung eine Gruppe von Objekten, die über eine gemeinsame Definition verfügen und aus diesem Grund mit denselben Merkmalen, Verarbeitungsoperationen und Funktionsweisen arbeiten.

Kryptographie
Bei der Sicherung von Computern die Prinzipien, Verfahren und Methoden zur Verschlüsselung von unverschlüsseltem und zur Entschlüsselung von verschlüsseltem Text.

L

LDAP
Lightweight Directory Access Protocol.

Lightweight Directory Access Protocol (LDAP)
Ein Protokoll, mit dem auf das Directory zugegriffen werden kann.

Liste der ausgestellten Zertifikate (ICL)
Eine vollständige Liste der ausgestellten Zertifikate sowie deren aktueller Status. Die Zertifikate sind anhand der Seriennummer und des Status indexiert. Diese Liste wird vom CA verwaltet und in der CA-Datenbank gespeichert.

M

MAC
Message Authentication Code - Nachrichtenauthentifizierungscode.

MD4
Eine Nachrichtenauszugs-Hash-Funktion auf 128-Bit-Basis, die von Ron Rivest entwickelt wurde. Ihre Geschwindigkeit übersteigt die von MD2 um ein Mehrfaches.

MD5
Eine unidirektionale Nachrichtenauszugs-Hash-Funktion, die von Ron Rivest entwickelt wurde. Sie stellt eine verbesserte Version von MD4 dar. MD5 verarbeitet Eingabetext in 512-Bit-Blöcken, die in 16 32-Bit-Unterblöcke aufgeteilt werden. Die Ausgabe des Algorithmus ist eine Gruppe von vier 32-Bit-Blöcken, die verkettet werden und so einen 128-Bit-Hash-Wert bilden. Diese Funktion wird ebenfalls zusammen mit MD2 in dem PEM-Protokollen verwendet.

MD2
Eine Nachrichtenauszugs-Hash-Funktion auf 128-Bit-Basis, die von Ron Rivest entwickelt wurde. Sie wird zusammen mit MD5 in den PEM-Protokollen verwendet.

Modulus
In dem auf öffentlichen Schlüsseln basierenden RSA-Verschlüsselungssystem das Produkt (n) aus zwei hohen Primzahlen: p und q. Die optimale Größe für einen RSA-Modulus hängt von den individuellen Sicherheitsanforderungen ab. Je größer der Modulus, desto höher die Sicherheit. Die momentan von den RSA Laboratories empfohlenen Schlüsselgrößen hängen vom geplanten Einsatz des Schlüssels ab. Hierbei werden 768 Bit für Schlüssel zum persönlichen Gebrauch, 1024 Bit für den

Unternehmensbereich und 2048 Bit für extrem wertvolle Schlüssel wie z. B. CA-Schlüsselpaare angegeben. Ein 768-Bit-Schlüssel wird voraussichtlich bis mindestens zum Jahr 2004 sicher sein.

Multipurpose Internet Mail Extensions (MIME)
Eine frei verfügbare Gruppe von Spezifikationen, die den Austausch von Text in Sprachen mit unterschiedlichen Zeichensätzen ermöglicht. Diese Spezifikationen unterstützen auch den Austausch von Multimedia-E-Mail zwischen unterschiedlichen Computersystemen, die Internet-Mail-Standards verwenden. So können E-Mail-Nachrichten beispielsweise andere Zeichensätze als den US-ASCII-Satz sowie erweiterten Text, Bilder oder Tondaten enthalten.

N

Nachrichtenauszug
Eine irreversible Funktion, bei der auf der Basis einer Nachricht beliebiger Länge eine Datenmenge mit fester Länge generiert wird. Bei MD5 handelt es sich z. B. um einen Nachrichtenauszugsalgorithmus.

Nachrichtenauthentifizierungscode (MAC)
Ein geheimer Schlüssel, der von Sender und Empfänger gemeinsam benutzt wird. Der Sender authentifiziert sich und der Empfänger prüft die hierbei zur Verfügung gestellten Daten. Bei Tivoli PKI werden MAC-Schlüssel für CA- und Prüfkomponenten in den KeyStores gespeichert.

National Security Agency (NSA)
Die offizielle Sicherheitsbehörde der US-Regierung.

NIST
National Institute of Standards and Technology, früher NBS (National Bureau of Standards). Aufgabe dieses Instituts ist die Unterstützung offener Standards und der Interoperabilität in den verschiedenen Bereichen der Computerbranche.

NLS
National Language Support - Unterstützung in der Landessprache.

NSA
National Security Agency.

O

Objekt
Beim objektorientierten Design oder bei der objektorientierten Programmierung eine abstrakte Entität, die zur Abgrenzung bestimmter Daten und der zugehörigen Operationen dient. *Siehe auch* Klasse.

Objektart
Die Art von Objekt, die im Directory gespeichert werden kann. Beispiele sind eine Firma, ein Konferenzraum, eine Einheit, eine Person, ein Programm oder ein Prozess.

Objekt-ID (OID)
Ein von einer Verwaltungsfunktion zugeordneter Datenwert, der den in ASN.1 definierten Typ aufweist.

ODBC
Open Database Connectivity.

Öffentlicher Schlüssel
In einem Paar aus einem öffentlichen und einem privaten Schlüssel steht dieser Schlüssel anderen Benutzern zur Verfügung. Er ermöglicht diesen Benutzern die Weiterleitung einer Transaktion an den Eigner des Schlüssels sowie die Prüfung einer digitalen Unterschrift. Mit einem öffentlichen Schlüssel verschlüsselte Daten können nur mit dem entsprechenden privaten Schlüssel entschlüsselt werden. *Gegensatz zu* Privater Schlüssel. *Siehe auch* Schlüsselpaar aus öffentlichem und privatem Schlüssel.

Open Database Connectivity (ODBC)
Ein Standard für den Zugriff auf unterschiedliche Datenbanksysteme.

Open Systems Interconnect (OSI)
Der Name der von ISO genehmigten Computernetzstandards.

OSI
Open Systems Interconnect.

P

PC-Karte
Eine mit einer Smart-Card vergleichbare Einheit, die auch als PCMCIA-Karte bezeichnet wird. Sie ist etwas größer als eine Smart-Card und verfügt im Allgemeinen über eine höhere Kapazität.

4758 PCI Cryptographic Coprocessor
Eine programmierbare, manipulationssensitive PCI-Bus-Verschlüsselungskarte, die die Ausführung von DES- und RSA-Verschlüsselungsoperationen mit hoher Geschwindigkeit ermöglicht. Die Verschlüsselungsprozesse werden in einem gesicherten und abgegrenzten Bereich auf der Karte ausgeführt. Die Karte entspricht den strengen Anforderungen des FIPS PUB 140-1 Level 4-Standards. In dem gesicherten und abgegrenzten Bereich kann Software ausgeführt werden. Der SET-Standard kann z. B. zur Verarbeitung von Kreditkartentransaktionen genutzt werden.

PEM
Privacy-Enhanced Mail.

PKCS
Public Key Cryptography Standards.

PKCS #1
Siehe Public Key Cryptography Standards.

PKCS #7
Siehe Public Key Cryptography Standards.

PKCS #10
Siehe Public Key Cryptography Standards.

PKCS #11
Siehe Public Key Cryptography Standards.

PKCS #12
Siehe Public Key Cryptography Standards.

PKI
Public Key Infrastructure.

PKIX
PKI auf X.509v3-Basis.

PKIX Certificate Management Protocol (PKIX CMP)
Ein Protokoll, das Verbindungen mit PKIX-kompatiblen Anwendungen ermöglicht. PKIX CMP verwendet als primäres Transportverfahren TCP/IP, es ist jedoch eine Abstraktionsebene oberhalb der Sockets-Schicht vorhanden. Dies ermöglicht die Unterstützung für zusätzliche Datenübertragungsoperationen mit Sendeaufrufen (Polling).

PKIX CMP
PKIX Certificate Management Protocol.

PKIX-Empfangseinheit
Der öffentliche HTTP-Server, der von einer bestimmten Registrierungsdomäne verwendet wird, um Anforderungen der Client-Anwendung von Tivoli PKI zu empfangen.

Privacy-Enhanced Mail (PEM)
Der vom Internet Architect Board (IAB) genehmigte Internet-Standard für die verbesserte Wahrung der Vertraulichkeit, der die sichere Übertragung elektronischer Post (E-Mail) über das Internet ermöglicht. Die PEM-Protokolle regeln Verschlüsselung, Authentifizierung, Nachrichtenintegrität und Schlüsselverwaltung.

Privater Schlüssel

In einem Paar aus einem öffentlichen und einem privaten Schlüssel steht dieser Schlüssel nur für seinen Eigner zur Verfügung. Er ermöglicht dem Eigner das Empfangen einer privaten Transaktion oder eine digitale Unterschrift. Die mit einem privaten Schlüssel unterzeichneten Daten können nur mit dem entsprechenden öffentlichen Schlüssel geprüft werden. *Gegensatz zu* öffentlicher Schlüssel. *Siehe auch* Schlüsselpaar aus öffentlichem und privatem Schlüssel.

Protokoll

Eine vereinbarte Konvention für die Kommunikation zwischen Computern.

Protokollierungssubsystem

Bei Tivoli PKI ein Subsystem, das die Unterstützungsfunktionen zum Protokollieren von sicherheitsrelevanten Aktionen bereitstellt. Es entspricht den Empfehlungen, die im X9.57-Standard unter *Public Key Cryptography for the Financial Services Industry* definiert wurden.

Proxy-Server

Eine Einheit, die zwischen einem Computer, der eine Zugriffsanforderung absetzt (Computer A) und einem Computer, auf den zugegriffen werden soll (Computer B), implementiert ist. Wenn ein Endbenutzer eine Anforderung für eine Ressource über Computer A absetzt, wird diese an den Proxy-Server geleitet. Dieser sendet die Anforderung an Computer B, erhält von diesem die Antwort und leitet diese an den Endbenutzer weiter. Mit Hilfe eines Proxy-Servers kann über einen Computer, der sich innerhalb einer Firewall befindet, auf das World Wide Web zugegriffen werden.

Prüf-Client

Jeder Client im System, der Prüfereignisse an den Tivoli PKI-Prüf-Server sendet. Bevor ein Prüf-Client ein Ereignis an den Prüf-Server sendet, stellt er eine Verbindung zu diesem her. Nach der Herstellung der Verbindung verwendet der Client die Client-Bibliothek des Prüfsubsystems, um Ereignisse an den Prüf-Server zu übertragen.

Prüfprotokoll

Daten in Form eines logischen Pfades, die eine Folge von Ereignissen verbinden. Mit dem Prüfprotokoll können Transaktionen oder der bisherige Verlauf einer bestimmten Aktivität verfolgt werden.

Prüfprotokoll

Bei Tivoli PKI eine Tabelle in einer Datenbank, in der für jedes Prüfereignis ein Datensatz gespeichert wird.

Prüf-Server

Ein Tivoli PKI-Server, der zum Empfangen von Prüfereignissen von Prüf-Clients und zum Aufzeichnen dieser Ereignis in einem Prüfprotokoll dient.

Prüfzeichenfolge

Eine Zeichenfolge, die von einem Server oder einer Anwendung gesendet wird und zum Anfordern der Benutzerberechtigung dient. Der Benutzer, der zur Authentifizierung aufgefordert wird, unterzeichnet die Prüfzeichenfolge mit einem privaten Schlüssel. Der öffentliche Schlüssel des Benutzers sowie die unterzeichnete Prüfzeichenfolge werden zurück an den Server oder die Anwendung gesendet, der bzw. die die Authentifizierung anforderte. Der Server versucht anschließend, die unterzeichnete Prüfzeichenfolge mit Hilfe des öffentlichen Schlüssels des Benutzers zu entschlüsseln. Wenn die entschlüsselte Prüfzeichenfolge mit der ursprünglich gesendeten Prüfzeichenfolge übereinstimmt, gilt der Benutzer als authentifiziert.

Public Key Cryptography Standards (PKCS)

Informelle, herstellerübergreifende Standards, die im Jahr 1991 von den RSA Laboratories in Zusammenarbeit mit Repräsentanten verschiedener Computerhersteller entwickelt wurden. Diese Standards umfassen die RSA-Verschlüsselung, die Diffie-Hellman-Vereinbarung, die kennwortbasierte Verschlüsselung sowie die Syntax für erweiterte Zertifikate, verschlüsselte Nachrichten, Daten zu privaten Schlüsseln und für die Zertifizierung.

- PKCS #1 beschreibt ein Verfahren zum Verschlüsseln von Daten mit Hilfe des RSA-Verschlüsselungssystems auf der Basis öffentlicher Schlüssel. Er dient zur Erstellung digitaler Unterschriften und Briefumschläge.
- PKCS #7 definiert ein allgemeines Format für verschlüsselte Nachrichten.
- PKCS #10 definiert eine Standardsyntax für Zertifizierungsanforderungen.
- PKCS #11 definiert eine Programmierschnittstelle für Verschlüsselungseinheiten, z. B. Smart-Cards, die unabhängig vom verwendeten technologischen Konzept ist.
- PKCS #12 definiert ein portierbares Format zum Speichern oder Transportieren der privaten Schlüssel, Zertifikate und sonstiger geheimer Daten etc. eines Benutzers.

Public Key Infrastructure (PKI)

Ein Standard für Sicherheitssoftware, der auf der Verschlüsselung mit Hilfe öffentlicher Schlüssel basiert. Bei PKI handelt es sich um ein System digitaler Zertifikate, Zertifikatsaussteller, Registrierungsstellen, Zertifikatverwaltungsservices und verteilter Verzeichnisservices. Er dient zum Prüfen der Identität und Berechtigung aller Parteien, die an Transaktionen beteiligt sind, die über das Internet ausgeführt werden. Diese Transaktionen umfassen möglicherweise Operationen, zu deren Ausführung eine Identitätsprüfung erforderlich ist. Sie dienen z. B. zur Bestätigung des Ursprungs von Senderechtanforderungen, E-Mail-Nachrichten oder Finanztransaktionen.

PKI stellt öffentliche Chiffrierschlüssel und Benutzerzertifikate für die Authentifizierung durch eine berechtigte Einzelperson oder ein berechtigtes Unternehmen zur Verfügung. Er stellt Online-Verzeichnisse bereit, die die öffentlichen Chiffrierschlüs-

sel und Zertifikate enthalten, die zur Überprüfung der digitalen Zertifikate, Identitätsnachweise sowie der digitalen Unterschriften verwendet werden.
PKI stellt außerdem Funktionen zur schnellen und effizienten Antwort auf Prüfabfragen und Anforderungen für öffentliche Chiffrierschlüssel bereit. Der Standard dient darüber hinaus zur Identifizierung potenzieller Sicherheitslücken im System und zur Verwaltung von Ressourcen zur Bearbeitung von Sicherheitsverletzungen. PKI bietet außerdem einen digitalen Zeitmarkenservice für wichtige Unternehmenstransaktionen.

R

RA

Registration Authority - Registrierungsstelle.

RA Desktop

Ein Java-Applet, das den RAs eine Grafikschnittstelle für die Verarbeitung von Anforderungen für Identitätsnachweise und zur Verwaltung dieser Nachweise während ihrer Gültigkeitsdauer zur Verfügung stellt.

RA-Server

Der Server für die RA-Komponente von Tivoli PKI.

RC2

Eine variable Schlüsselgrößen-Block-Cipher, die von Ron Rivest für RSA Data Security entwickelt wurde. *RC* steht für *Ron's Code* oder *Rivest's Cipher*. Sie arbeitet schneller als DES und löst diese Block-Cipher ab. Durch die Verwendung geeigneter Schlüsselgrößen kann sie in Bezug auf eine ausgedehnte Schlüsselsuche flexibler als DES gestaltet werden. Sie verfügt über eine Blockgröße von 64 Bit und arbeitet auf Softwareebene zwei- bis dreimal schneller als DES. RC2 kann in denselben Modi eingesetzt werden wie DES.
Durch eine Vereinbarung zwischen SPA (Software Publishers Association) und der US-Regierung nimmt RC2 einen speziellen Status ein. Hierdurch ist das Genehmigungsverfahren für den Export einfacher und schneller, als dies bei anderen Verschlüsselungsprodukten der Fall ist. Um die Voraussetzungen für eine rasche Exportgenehmigung zu erfüllen, muss ein Produkt mit einigen Ausnahmen die RC2-Schlüsselgröße auf 40 Bit beschränken. Eine zusätzliche Zeichenfolge kann verwendet werden, um Nichtberechtigte abzuwehren, die versuchen, eine umfangreiche Tabelle möglicher Verschlüsselungsvarianten vorauszuberechnen.

Regel-Exit

In einer Registrierungsfunktion ein auf Unternehmensebene definiertes Programm, das von der Registrierungsanwendung aufgerufen wird. Die Regeln eines Regel-Exits implementieren die Unternehmens- und Sicherheitsbenutzervorgaben eines Unternehmens für den Registrierungsprozess.

Registrierter Name (DN)
Der eindeutige Name eines im Directory gespeicherten Dateneintrags. Der DN dient zur eindeutigen Identifizierung der Position eines Eintrags in der hierarchischen Struktur des Directory.

Registrierung
Bei Tivoli PKI das Abrufen von Identitätsnachweisen für die Verwendung über das Internet. Bei der Registrierung werden Zertifikate angefordert, erneuert und widerrufen.

Registrierungsattribut
Eine Registrierungsvariable, die in einem Registrierungsformular enthalten ist. Ihr Wert gibt die Informationen wider, die während der Registrierung erfasst werden. Der Wert des Registrierungsattributs bleibt während der gesamten Gültigkeitsdauer des Identitätsnachweises gleich.

Registrator
Ein Benutzer, der für den Zugriff auf RA Desktop sowie zur Verwaltung und Anforderung von Zertifikaten berechtigt ist.

Registrierungsstelle (RA)
Die Software, die zur Verwaltung digitaler Zertifikate verwendet wird und sicherstellt, dass die Unternehmensregeln vom ersten Empfang einer Registrierungsanforderung bis zum Zertifikatswiderruf angewendet werden.

Registrierungsdatenbank
Diese Datenbank enthält Informationen zu Zertifikatsanforderungen und ausgestellten Zertifikaten. In der Datenbank werden Registrierungsdaten gespeichert und alle Änderungen aufgezeichnet, die während der Gültigkeitsdauer an einem Zertifikat vorgenommen werden. Die Datenbank kann durch RA-Prozesse und Regel-Exits oder durch den Registrator aktualisiert werden.

Registrierungsdomäne
Eine Gruppe von Ressourcen, Regeln und Konfigurationsoptionen, die sich auf bestimmte Registrierungsprozesse für Zertifikate beziehen. Der Domänenname stellt einen untergeordneten Wert zur URL-Adresse dar, die zur Ausführung der Registrierungsfunktion eingesetzt wird.

Registrierungsfunktion
Ein Tivoli PKI-Anwendungsgerüst, das spezielle Verfahren zur Registrierung von Entitäten (z. B. Browser, Router, E-Mail-Einheiten und sichere Client-Anwendungen) und zur Verwaltung von Zertifikaten während ihrer Gültigkeitsdauer bereitstellt.

Registrierungsprozess
Bei Tivoli PKI die Schritte, die zur Überprüfung eines Benutzers ausgeführt werden. Durch den Registrierungsprozess werden Benutzer sowie deren öffentliche Schlüssel zertifiziert, um sie zur Teilnahme an den gewünschten Transaktionen zu berechtigen.

Er kann lokal oder Web-gestützt, automatisch oder von einer tatsächlich mit Personen besetzten Registrierungsstelle ausgeführt werden.

Registrierungsvariable
Siehe Registrierungsattribut.

RSA
Ein auf öffentlichen Schlüsseln basierender Verschlüsselungsalgorithmus, der nach seinen Erfindern (Rivest, Shamir und Adelman) benannt wurde. Er wird zur Verschlüsselung und für digitale Unterschriften verwendet.

S

Schema
Beim Directory die interne Struktur, die zur Definition der Beziehungen zwischen den verschiedenen Objektarten verwendet wird.

Schlüssel
Bei der Verschlüsselung ein Wert, der zum Ver- und Entschlüsseln von Informationen verwendet wird.

Schlüsselpaar
Zusammengehörende Schlüssel, die bei der asymmetrischen Verschlüsselung eingesetzt werden. Ein Schlüssel wird zur Verschlüsselung, der andere zur Entschlüsselung verwendet.

Schlüsselpaar aus öffentlichem und privatem Schlüssel
Ein Schlüsselpaar aus öffentlichem und privatem Schlüssel stellt ein grundlegendes Element der Verschlüsselung auf der Basis von Schlüsselpaaren dar. (Diese Form der Verschlüsselung wurde im Jahr 1976 von Whitfield Diffie und Martin Hellman eingeführt, um Probleme bei der Schlüsselverwaltung zu lösen.) Nach diesem Konzept erhält jeder Benutzer ein Schlüsselpaar, bei dem einer als öffentlicher und einer als privater Schlüssel bezeichnet wird. Der öffentliche Schlüssel ist hierbei allgemein bekannt, der private Schlüssel wird hingegen geheim gehalten. Sender und Empfänger müssen geheime Daten nicht gemeinsam benutzen. Alle Kommunikationsoperationen werden lediglich auf der Basis öffentlicher Schlüssel ausgeführt. Die privaten Schlüssel werden niemals übertragen oder gemeinsam verwendet. Auf diese Weise ist es nicht mehr notwendig, sich auf die Sicherheit eines Übertragungskanals gegenüber Manipulationen zu verlassen. Die einzige Anforderung ist, dass öffentliche Schlüssel den entsprechenden Benutzern in einer gesicherten (authentifizierten) Weise (z. B. in einem gesicherten Verzeichnis) zugeordnet werden. Jeder Benutzer kann nun mit Hilfe dieser öffentlichen Daten eine vertrauliche Nachricht senden. Diese Nachricht kann nur mit einem privaten Schlüssel entschlüsselt werden, auf den allein der gewünschte Empfänger zugreifen kann. Darüber hinaus kann die Verschlüsselung auf der Basis von Schlüsselpaaren nicht nur zur

Gewährleistung der Vertraulichkeit (Verschlüsselung), sondern auch für die Authentifizierung (digitale Unterschriften) eingesetzt werden.

Schlüsselsicherung und -wiederherstellung
Diese Funktion von Tivoli PKI ermöglicht das Sichern und Wiederherstellen von Endentitätszertifikaten und der zugehörigen, von Tivoli PKI zertifizierten öffentlichen und privaten Schlüssel. Die Zertifikate und Schlüssel werden in einer PKCS #12-Datei gespeichert. Diese Datei ist kennwortgeschützt. Das Kennwort wird beim Sichern des Zertifikats und der Schlüssel gesetzt.

Secure Electronic Transaction (SET)
Ein Branchenstandard für die Durchführung sicherer Kredit- oder Kundenkartenzahlungen über nicht gesicherte Netze. Der Standard formuliert Definitionen für die Authentifizierung von Kartenhaltern, Händlern sowie der Banken, durch die die Karten ausgestellt werden, da er die Ausstellung von Zertifikaten anfordert.

Secure Sockets Layer (SSL)
Ein IETF-Standardübertragungsprotokoll mit integrierten Sicherheitsservices, die für den Endbenutzer möglichst transparent sind. Es stellt einen digitalen, sicheren Kommunikationskanal zur Verfügung.
Ein SSL-fähiger Server empfängt SSL-Verbindungsanforderungen im Allgemeinen an einem anderen Anschluss (Port) als normale HTTP-Anforderungen. SSL erstellt eine Sitzung, in der die Austauschsignale zum Herstellen der Kommunikation zwischen zwei Modems nur einmal gesendet werden müssen. Anschließend wird die Kommunikation verschlüsselt und die Nachrichtenintegrität wird solange überprüft, bis die SSL-Sitzung abgelaufen ist.

Server
(1) In einem Netz eine Datenstation, die anderen Stationen Funktionen zur Verfügung stellt, wie beispielsweise ein Datei-Server. (2) In TCP/IP ein System in einem Netz, das die Anforderungen eines Systems an einem anderen Standort verarbeitet. Dieses Konzept wird als Client/Server-Modell bezeichnet.

Server-Zertifikat
Ein digitales Zertifikat, das von einem CA ausgegeben wird und es einem Web-Server ermöglicht, SSL-gestützte Transaktionen auszuführen. Wenn ein Browser über das SSL-Protokoll eine Verbindung zum Server herstellt, sendet der Server seinen öffentlichen Schlüssel an den Browser. Hierdurch kann die Identität des Servers authentifiziert werden und es können verschlüsselte Daten an den Server gesendet werden. *Siehe auch* CA-Zertifikat, Digitales Zertifikat *und* Browserzertifikat.

Servlet
Ein Server-Programm, das zusätzliche Funktionen für Server zur Verfügung stellt, die Java unterstützen.

SET
Secure Electronic Transaction.

SGML
Standard Generalized Markup Language.

SHA-1 (Secure Hash Algorithm)
Ein von NIST und NSA entwickelter Algorithmus, der beim DSS (Digital Signature Standard) verwendet wird. Der Standard wird als Secure Hash Standard bezeichnet; SHA ist der Algorithmus, der von diesem Standard verwendet wird. Er generiert einen 160-Bit-Hash-Code.

Sicherheitsdomäne
Eine Gruppe (z. B. Unternehmen, Arbeitsgruppe, Projektteam), deren Zertifikate vom gleichen CA zertifiziert wurden. Benutzer, die über ein von einem CA unterzeichnetes Zertifikat verfügen, können der Identität eines anderen Benutzers vertrauen, der ein Zertifikat besitzt, das vom selben CA unterzeichnet worden ist.

Sicherungsmodell
Eine Organisationskonvention, die regelt, wie Zertifikatsaussteller (CAs) andere Zertifikatsaussteller zertifizieren können.

Simple Mail Transfer Protocol (SMTP)
Ein Protokoll, mit dem elektronische Post über das Internet übertragen wird.

Site-Zertifikat
Dieser Zertifikatstyp ist mit einem CA-Zertifikat vergleichbar, gilt jedoch nur für eine bestimmte Website. *Siehe auch* CA-Zertifikat.

Smart-Card
Eine Hardwarekomponente, normalerweise in der Größe einer Kreditkarte, auf der die digitalen Schlüssel eines Benutzers gespeichert werden können. Eine Smart-Card kann kennwortgeschützt werden.

S/MIME
Ein Standard, der das Unterzeichnen und Verschlüsseln von elektronischer Post (E-Mail) unterstützt, die über das Internet übertragen wird. *Siehe* MIME.

SMTP
Simple Mail Transfer Protocol.

SSL
Secure Sockets Layer.

Standard Generalized Markup Language (SGML)
Ein Standard zur Beschreibung von Formatierungssprachen. HTML basiert auf SGML.

Symmetrischer Schlüssel
Ein Schlüssel, der sowohl für die Verschlüsselung als auch für die Entschlüsselung verwendet werden kann. *Siehe auch* Symmetrische Verschlüsselung.

Symmetrische Verschlüsselung
Eine Form der Verschlüsselung, bei der sowohl für die Ver- als auch für die Entschlüsselung derselbe Schlüssel verwendet wird. Die Sicherheit dieses Verfahren basiert auf dem Schlüssel. Wird dieser öffentlich bekannt gegeben, können die mit ihm bearbeiteten Nachrichten von jedem Benutzer ver- und entschlüsselt werden. Der Inhalt der übertragenen Daten kann nur dann geheim gehalten werden, wenn der Schlüssel nur den jeweils berechtigten Personen bekannt ist. *Gegensatz zu* Asymmetrische Verschlüsselung.

T

TCP/IP
Transmission Control Protocol/Internet Protocol.

TP
Trust Policy = Sicherungsregel.

Transaktions-ID
Eine Kennung, die die RA als Antwort auf eine Anforderung für eine Vorabregistrierung zur Verfügung stellt. Mit dieser ID kann ein Benutzer, der die Client-Anwendung von Tivoli PKI ausführt, ein vorab genehmigtes Zertifikat erhalten.

Transmission Control Protocol/Internet Protocol (TCP/IP)
Eine Gruppe von Übertragungsprotokollen, die Peer-zu-Peer-Konnektivitätsfunktionen für lokale Netze (LANs) und Weitverkehrsnetze (WANs) unterstützen.

Triple DES
Ein symmetrischer Algorithmus, bei dem der unverschlüsselte Text dreimal verschlüsselt wird. Obwohl für diese Mehrfachverschlüsselung zahlreiche Methoden existieren, stellt die Triple DES-Verschlüsselung, die auf drei verschiedenen Schlüsseln basiert, das sicherste dieser Verfahren dar.

Tivoli PKI
Eine integrierte IBM Sicherheitslösung, die die Ausstellung, Erneuerung und den Widerruf digitaler Zertifikate unterstützt. Diese Zertifikate können für eine breite Palette von Internet-Anwendungen eingesetzt werden und bieten eine Möglichkeit zur Authentifizierung von Benutzern und zur Gewährleistung einer gesicherten Kommunikation.

Trust-Kette
Eine Gruppe von Zertifikaten, die aus der gesicherten Hierarchie vom Benutzerzertifikat bis zum Root- oder selbstunterzeichneten Zertifikat besteht.

Tunnel
In der VPN-Technologie eine virtuelle Punkt-zu-Punkt-Verbindung, die auf Anfrage über das Internet hergestellt wird. Während der Verbindung können ferne Benutzer

den Tunnel verwenden, um sichere, verschlüsselte und gekapselte Informationen mit Servern im privaten Netz eines Unternehmens auszutauschen.

U

Unbestreitbarkeit
Die Verwendung eines digitalen, privaten Schlüssels, um zu verhindern, dass der Unterzeichner eines Dokuments dessen Unterzeichnung leugnet.

Unicode
Ein 16-Bit-Zeichensatz, der in ISO 10646 definiert ist. Der Unicodestandard für die Verschlüsselung von Zeichen ist ein internationaler Zeichencode für die Informationsverarbeitung. Er umfasst die grundlegenden, weltweit verwendeten Prozeduren und bildet die Basis für die Internationalisierung und Lokalisierung von Software. Der gesamte Quellencode in der Java-Programmierungsumgebung wird in Unicode geschrieben.

Unternehmensprozessobjekte
Eine Codegruppe, die zur Ausführung einer bestimmten Registrierungsoperation, z. B. zum Prüfen des Registrierungsstatus oder zur Bestätigung des Sendens eines öffentlichen Schlüssels, verwendet wird.

Unternehmensprozessschablone
Eine Gruppe von Unternehmensprozessobjekten, die in einer bestimmten Reihenfolge ausgeführt werden.

Unterstützung in der Landessprache (NLS)
Unterstützung für unterschiedliche länderspezifische Angaben in einem Produkt. Hierzu gehören die Sprache, die Währung, das Datums- und Zeitformat und die Darstellung von Zahlen.

Unterzeichnen
Die Verwendung eines digitalen privaten Schlüssels zum Generieren einer Unterschrift. Diese Unterschrift dient dazu, zu beweisen, dass ein bestimmter Benutzer für die von ihm unterzeichnete Nachricht verantwortlich ist und diese akzeptiert.

Unterzeichnen/Prüfen
Als Unterzeichnen wird die Verwendung eines privaten Schlüssels zum Generieren einer Unterschrift bezeichnet. Unter Prüfen versteht man die Verwendung des entsprechenden öffentlichen Schlüssels zur Verifizierung dieser Unterschrift.

Unverschlüsselter Text
Nicht verschlüsselte Daten. *Synonym zu* Klartext.

URL
Uniform Resource Locator - URL-Adresse.

URL-Adresse

Ein Schema für die Adressierung von Ressourcen im Internet. Die URL-Adresse gibt das verwendete Protokoll sowie den Host-Namen und die IP-Adresse an. Außerdem enthält er Angaben zur Anschlussnummer, zum Pfad sowie weitere Ressourcendetails, die erforderlich sind, um über eine bestimmte Maschine auf eine Ressource zuzugreifen.

UTF-8

Ein Umsetzungsformat. Es ermöglicht Informationsverarbeitungssystemen, die nur die Verarbeitung von 8-Bit-Zeichensätzen unterstützen, die Umsetzung von 16-Bit-Unicode in ein 8-Bit-Äquivalent und umgekehrt, ohne dass hierbei Informationen verloren gehen.

V

Verkettungsprüfung

Die Gültigkeitsprüfung aller CA-Unterschriften in der Trust-Hierarchie, über die ein bestimmtes Zertifikat ausgestellt wurde. Wenn z. B. das Unterschriftszertifikat eines CA über einen anderen CA ausgestellt wurde, werden bei der Gültigkeitsprüfung des vom Benutzer vorgelegten Zertifikats beide Unterschriften geprüft.

Verschlüsseln

Das Umordnen von Informationen, so dass nur Personen, die über den richtigen Entschlüsselungscode verfügen, die ursprünglichen Informationen durch Entschlüsselung abrufen können.

Verschlüsselt

Die Eigenschaft von Daten, die nach einem bestimmten System umgesetzt wurden, um deren Bedeutung unkenntlich zu machen.

Verschlüsselung/Entschlüsselung

Die Verwendung des öffentlichen Schlüssels des gewünschten Empfängers zum Verschlüsseln von Daten für diese Person. Der Empfänger verwendet anschließend den privaten Schlüssel seines Schlüsselpaares, um die Daten zu entschlüsseln.

Vertrauensdomäne

Eine Gruppe von Entitäten, deren Zertifikate vom gleichen CA zertifiziert wurden.

Vertraulichkeit

Der Schutz von Daten gegen den Zugriff nicht berechtigter Personen.

Vertraulichkeit

Die Wahrung der Geheimhaltung bestimmter Informationen gegenüber nicht berechtigten Personen.

Virtual Private Network (VPN)

Ein privates Datennetz, das ferne Verbindungen nicht über Telefonleitungen, sondern über das Internet herstellt. Da der Zugriff der Benutzer auf die Netzressourcen eines Unternehmens nicht über eine Telefongesellschaft, sondern über einen Internet Service Provider (ISP) erfolgt, können diese durch den Einsatz von VPN deutliche Einsparungen bei Fernzugriffen erzielen. Ein VPN erhöht auch die Sicherheit beim Datenaustausch. Bei der herkömmlichen Firewall-Technologie kann zwar der Inhalt der Nachricht verschlüsselt werden, nicht jedoch die Quellen- und Zieladressen. Bei der VPN-Technologie können die Benutzer eine Tunnelverbindung herstellen, bei der das gesamte Datenpaket (Header- und Datenkomponente) verschlüsselt und gekapselt ist.

Vorabregistrierung

Bei Tivoli PKI ein Prozess, mit dem ein bestimmter Benutzer (normalerweise ein Administrator) andere Benutzer registrieren kann. Wenn die Anforderung genehmigt wird, stellt die RA Informationen zur Verfügung, mit denen der Benutzer später mit Hilfe der Client-Anwendung von Tivoli PKI ein Zertifikat erhalten kann.

VPN

Virtual Private Network.

W

Web-Browser

Auf einem PC ausgeführte Client-Software, mit der ein Benutzer im World Wide Web navigieren oder lokale HTML-Seiten anzeigen kann. Der Web-Browser ist ein Abfrage-Tool, das universellen Zugriff auf die umfangreichen Hypermedia-Datensammlungen ermöglicht, die im Web und im Internet zur Verfügung gestellt werden. Manche Browser können Text und Grafik anzeigen, während andere Browser auf die Textanzeige beschränkt sind. Die meisten Browser unterstützen die Hauptformen der Internet-Kommunikation, z. B. die Ausführung von FTP-Transaktionen.

Web-Server

Ein Server-Programm, das auf Anforderungen von Browser-Programmen nach Informationsressourcen antwortet. *Siehe auch* Server.

WebSphere Application Server

Ein IBM Produkt, das Benutzer bei der Entwicklung und Verwaltung von Websites mit einem hohen Leistungsumfang unterstützt. Es erleichtert den Übergang vom einfachen Web Publishing zu komplexen e-business-Anwendungen im Web. Der WebSphere Application Server besteht aus einer Java-Servlet-Maschine, die unabhängig vom Webserver und dem verwendeten Betriebssystem arbeitet.

World Wide Web (WWW)

Der Teil des Internets, in dem ein Netz von Verbindungen zwischen Computern aufgebaut wird, auf denen Hypermediamaterial gespeichert ist. Dieses Material stellt

neben Informationen auch Verbindungen (Hyperlinks) zu anderem Material im World Wide Web und Internet zur Verfügung. Der Zugriff auf WWW-Ressourcen erfolgt über einen Web-Browser.

X

X.500

Ein Standard für die Implementierung eines multifunktionalen, verteilten und vervielfältigten Verzeichnisservices durch die Verbindung von Computersystemen. Dieser Standard wurde gemeinsam definiert von der bisher als CCITT bekannten International Telecommunications Union (ITU) sowie der International Organization for Standardization und der International Electro-Chemical Commission (ISO/IEC).

X.509 Version 3-Zertifikat

Das X.509v3-Zertifikat verfügt über erweiterte Datenstrukturen für die Speicherung und das Abrufen von Informationen zu Zertifikatsanträgen, zur Zertifikatsverteilung und zu Zertifikatswiderrufen sowie zu Sicherheitsregeln und digitalen Unterschriften.

X.509v3-Prozesse dienen zum Erstellen von CRLs mit Zeitmarken für alle Zertifikate. Bei jeder Verwendung eines Zertifikats ermöglichen die X.509v3-Funktionen der Anwendung, die Gültigkeit des Zertifikats zu überprüfen. Die Anwendung kann außerdem feststellen, ob sich das Zertifikat auf der Zertifikatswiderrufsliste (CRL) befindet. CRLs unter X.509v3 können für eine bestimmte Gültigkeitsperiode erstellt werden. Sie können auch auf anderen Kriterien basieren, die zur Aufhebung der Gültigkeit eines Zertifikats führen. Wenn z. B. ein Mitarbeiter ein Unternehmen verlässt, wird sein Zertifikat in der CRL eingetragen.

X.509-Zertifikat

Ein weit verbreiteter Zertifikatsstandard, der entwickelt wurde, um die sichere Verwaltung und Verteilung von digital unterzeichneten Zertifikaten über sichere Internet-Netze zu unterstützen. Das X.509-Zertifikat definiert Datenstrukturen, die Prozeduren für die Verteilung öffentlicher Schlüssel unterstützen, die von zuverlässigen Stellen digital unterzeichnet sind.

Z

Zertifikatsaussteller (CA)

Die Software, die zur Einhaltung der Sicherheitsregeln eines Unternehmens und zur Vergabe gesicherter elektronischer Identitäten in Form von Zertifikaten dient. Der CA verarbeitet die Anforderungen von RAs zum Ausstellen, Erneuern und Widerrufen von Zertifikaten. Er kooperiert mit der RA, um Zertifikate und CRLs im Directory zu publizieren. *Siehe auch* Digitales Zertifikat.

Zertifikatserweiterung

Eine Zusatzfunktion des X.509v3-Zertifikatformats, die zur Einbindung zusätzlicher Felder in das Zertifikat dient. Es stehen Standard- und benutzerdefinierte Erweiterungen zur Verfügung. Die Standarderweiterungen dienen verschiedenen Zwecken und umfassen Schlüssel- und Regelinformationen, Betreff- und Ausstellerattribute sowie Einschränkungen, die für den Zertifizierungspfad gelten.

Zertifikatsprofil

Eine Gruppe von Kenndaten, die den gewünschten Zertifikatstyp definieren (z. B. SSL- oder IPSec-Zertifikate). Das Profil vereinfacht die Zertifikatsspezifikation und -registrierung. Der Aussteller kann die Namen der Profile ändern und Kenndaten des gewünschten Zertifikats angeben. Hierzu zählen z. B. der Gültigkeitszeitraum, die Verwendung von Schlüsseln, DN-Einschränkungen usw.

Zertifikatsregel

Eine benannte Gruppe mit Regeln, die angibt, ob ein Zertifikat für eine bestimmte Klasse von Anwendungen mit gemeinsamen Sicherheitsanforderungen anwendbar ist. Eine Zertifikatsregel kann z. B. angeben, ob ein bestimmter Zertifizierungstyp dem Benutzer die Ausführung von Transaktionen für Waren innerhalb eines bestimmten Preisbereichs ermöglicht.

Zertifikatswiderrufsliste (CRL)

Eine digital unterzeichnete, mit Zeitmarken versehene Liste der Zertifikate, die vom Zertifikatsaussteller (CA) widerrufen wurden. Die Zertifikate in dieser Liste sollten als nicht akzeptierbar behandelt werden. *Siehe auch* Digitales Zertifikat.

Zertifizierung

Der Prozess, bei dem eine zuverlässige, an der Kommunikation nicht beteiligte Stelle (der Zertifikatsaussteller - CA) einen elektronischen Identitätsnachweis ausstellt, der für die Identität einer Person, eines Unternehmens oder einer Organisation bürgt.

Ziel

Eine benannte oder ausgewählte Datenquelle.

Zugriffssteuerungsliste (ACL)

Ein Verfahren, mit dem die Verwendung einer bestimmten Ressource auf berechtigte Benutzer beschränkt werden kann.

Index

A

AIX
- Backup-Dienstprogramm 92
- Betriebssystemversion 27
- Boot-Werte 86, 111
- CD-ROM-Dateisystem 63
- cfguser, Benutzername 43, 90, 115
- Dateien prüfen 59
- Dateisysteme 61
- Datenträgergruppen 61
- Directory-Server installieren 67
- Hardwarekonfigurationen 30
- Host-Namensauflösung 63
- IBM 4758 PCI Cryptographic Coprocessor installieren 77
- Installationsabschluss, Prüfliste 91
- Installationsrichtlinien 77
- Installationsübersicht 57
- Konfiguration 58
- Serverplattformen 27
- Sicherheitsaspekte 40
- Sichern 64
- Softwarevoraussetzungen 27
- Systemabbild 64
- Systembenutzer 63
- Überlegungen zur Firewall 41
- Zugriffssteuerung 41

AIX/6000, Betriebssystem 27
Allgemeine Erweiterungen 25
Anpassung
- Regel-Exits 9
- Registrierungsdomäne 8
- Übersicht 126
- Zertifikatserweiterungen 25
- Zertifikatsprofile 8
- Zugriff 126

Architektur
- LDAP-Protokoll 20
- Objektspeicher 20

Architektur *(Forts.)*
- PKIX CMP-Protokoll 19

B

Benutzerhandbuch
- Übersicht 125
- Zugriff 125

Betriebssysteme
- für AIX-Server 27
- für NT-Server 27
- für Setup Wizard 31, 37

Bibliothek, Tivoli PKI-Website xii
Boot-Werte
- unter AIX 86
- unter Windows NT 111

Browser-Zertifikate 6

C

CD-ROM-Dateisystem 63
CD-ROMs, Produkt 55
CDSA 19
cfgPostInstall, Programm 90
cfguser, Benutzername 43, 90, 98, 115
Chiffrieralgorithmen 54
Client-Anwendung
- Dokumentation 125
- installieren 78, 108
- Systemvoraussetzungen 32

Client-Authentifizierung 44
Codeunterzeichnung 21
Common Data Security Architecture (CDSA) 19
createconfig_start.sql, Datei 86, 111

CRL 10

D

datavg, Datenträgergruppe 61
Dateisysteme
  CD-ROM 63
  für den AIX-Server 61
  prüfen 59
Dateisysteme, unter AIX konfigurieren 61
Datenbanken
  CA-Daten 10
  Directory-Daten 15
  Installationsrichtlinien 64
  Prüfdaten 12
  Registrierungsdatum 5
  reservierte Namen 43
  Schlüssel sichern und wiederherstellen 17
  Systemvoraussetzungen 28
  Übersicht 14
Datenträgergruppen, unter AIX konfigurieren 61
DB2
  CA-Datenbank 10
  Datenverschlüsselung 22
  db2admin-Benutzer 99
  Directory-Datenbank 15
  Installation 65
  Prüfdatenbank 12
  reservierte Namen 43
  Systemvoraussetzungen 28
  unter AIX installieren 64, 65
  unter Windows NT installieren 99
  Vorteile 14
db2admin-Benutzer 99
Definition von Plattenpartitionen unter AIX 61
Directory-Administrator
  DN-Eintrag 48
  Schlüsselspeicher (KeyStore) 22
Directory-Schema 47
Directory-Server
  CA-DN 48
  Directory-Administrator, registrierter Name 48
  Konfiguration 46
Directory-Server *(Forts.)*
  Root-DN 48
  Schema 47
  Softwarevoraussetzungen 28
  Übersicht 15
  unter AIX installieren 67, 79
  unter Tivoli PKI verwenden 107
  unter Windows NT installieren 105, 109
  Zugriffssteuerung 48
DN, definiert 47
DNS 45, 46
Domestic Encryption Edition 54
DOS-Umgebung 116

E

Einschränkungen, Serverkonfiguration 53
Erste Schritte
  Konfiguration 119
  mit Anpassung 126
  RA-Verwaltung 123
  Registrierung 125
  Systemverwaltung 122
  Tivoli PKI 121
Exportierbarkeit, Chiffrieralgorithmen 54

F

Firewall-Sicherheit 41
FirstSecure
  Integration mit dem Policy Director 51
  Planung und Integration 51

G

Gegenseitige Zertifizierung 11
Größe von Plattenpartitionen unter AIX 61
Gruppen von Datenträgern, unter AIX konfigurieren 61

H

Handbuchzielgruppe xii
Hardware Security Model (HSM) 16
Hardwarevoraussetzungen
  IBM 4758 PCI Cryptographic Coprocessor 28
  Server, erforderlich 29
  Server, wahlfrei 28
  Setup Wizard 31
Hauptspeicher (Arbeitsspeicher)
  für AIX empfohlen 30
  für Windows NT empfohlen 30
Hierarchie, CA 11
Hilfe
  für die Registrierung 125
  für RA Desktop 124
  für Setup Wizard 120
Host-Namensauflösung, AIX 63
Hostname, für TCP/IP angeben 59
HSM-Einheit 16
HTTP-Protokoll 44
httpd.conf, Datei 90, 115
HTTPS-Protokoll 44

I

IBM 4758 PCI Cryptographic Coprocessor
  CA-Schlüsselspeicher (KeyStore) 22
  CA-Unterstützung 11, 15
  installieren 50, 77
  Integration in den CA 49
  Konfiguration 49
  Speichern des CA-Schlüssels 50
  Systemvoraussetzungen 28
  Übersicht 15
  Verschlüsseln des CA-Schlüssels 49
IBM HTTP Server
  unter AIX installieren 72
  unter Windows NT installieren 101, 102
ICL 10
Informationen zu diesem Handbuch xi
Installation
  AIX 58
Installation *(Forts.)*
  bestätigen, Windows NT-System 107
  Datenbanksoftware unter AIX 64, 65
  Datenbanksoftware unter Windows NT 99
  Directory-Server unter AIX 67
  Directory-Server unter Windows NT 105
  HTTP-Server unter Windows NT 102
  IBM 4758 PCI Cryptographic Coprocessor unter AIX 50, 77
  JDK unter Windows NT 101
  Prüfliste für den Installationsabschluss, AIX 91
  Prüfliste für den Installationsabschluss, Windows NT 116
  Server-Komponenten unter AIX 77
  Server-Komponenten unter Windows NT 108
  Web-Server unter AIX 72
  Web-Server unter Windows NT 101
  WebSphere Application Server unter AIX 72
  WebSphere Application Server unter Windows NT 104
  Windows NT 96
Installationsabschluss, Konfigurationsprogramm 90, 115
Installationsplanungsprüfliste 34
installp, Programm 79
InstallShield, Server-Konfiguration 109
Integritätsschutz
  von CA-Sätzen 10
  von Prüfsätzen 13
International Encryption Edition 54
IP-Aliasnamen
  Beschreibung 44
  unter Windows NT definieren 105
IPSec-Zertifikate 6

J

Java
  unter AIX installieren 70
JDK
  erforderliche Version 28
  unter Windows NT installieren 101

K

Kennwörter
- für AIX-Server 27
- für NT-Server 27
- für Setup Wizard 31, 37

KeyWorks installieren 78
Konfiguration
- AIX-Dateisysteme 61
- AIX-Datenträgergruppen 61
- Boot-Werte unter Windows NT 86, 111
- Directory-Server 46
- DOS-Umgebungskonfiguration 116
- Firewalls 41
- Formular für die Datenerfassung 92, 116
- Server-Architektur 53
- Übersicht 119
- Übersicht über den Prozess 119
- unter AIX vorbereiten 91, 119
- unter Windows NT vorbereiten 116, 119
- Web-Server 44
- Zugriff 120

Konfigurationsdatenformular 92, 116
Konfigurationsprogramm, Server-Software 109
Konventionen xvi
Kundenunterstützung xvi

L

Liste der ausgestellten Zertifikate (ICL) 10

M

MACs
- für CA-Sätze 10
- für Prüfsätze 13
- in Schlüsselspeichern (KeyStores) 22

Maschinentypen
- für AIX empfohlen 30
- für Windows NT empfohlen 30

Masken für Prüfereignisse 12
Massenausstellung von Zertifikaten
- Beschreibung 18

Migration
- Backup-Dienstprogramm unter AIX 92
- Backup-Dienstprogramm unter Windows NT 117

N

Nachrichtenunterzeichnung 21
Name, TCP/IP-Host angeben 59
Netfinity-Server 29
Netzsicherheit 40

O

Objektspeicher 20
Öffentlicher Web-Server 44

P

Physische Sicherheit 40
PKCS #12-Datei wiederherstellen 17
PKI, Definition 18
PKIX, Definition 19
PKIX CMP-Zertifikate 6
Planungsprüfliste, Installation 34
Plattenpartitionen
- dbfsadt 62
- dbfsibm 62
- dbfskrb 62
- dbfspkrf 62
- für den AIX-Server 61

Plattenspeicherplatz
- für AIX empfohlen 30
- für Windows NT empfohlen 30
- Größe, Richtlinien 29, 61

Policy Director 51
Private Erweiterungen 25

Produktpaket 55
Protokolle
  HTTP 44
  HTTPS 44
  LDAP 20
  PKIX CMP 19
  SSL 44
  unter Tivoli PKI unterstützt 23
Prozessoren
  für AIX empfohlen 30
  für Windows NT empfohlen 30
Prüfen des Hostnamens 59
Prüfliste, Installationsplanung 34
Prüflisten
  Installationsabschluss unter AIX 91
  Installationsabschluss unter Windows NT 116
Prüfsubsystem
  archivieren 13
  Datenbank 12
  Ereignismasken 12
  Integritätsprüfung 13
  MACs 13
  Schlüsselspeicher (KeyStore) 22
  Übersicht 12
  unter AIX installieren 79
  unter Windows NT installieren 109

R

RA Desktop
  Dokumentation 123
  Hilfe 124
  installieren 78, 108
  Registratoren hinzufügen 7
  Systemvoraussetzungen 32
  Übersicht 7, 123
  verwenden 123
  Zugriff 124
Regel-Exits
  Anpassung 9
  Definition 6
Registratoren 7
Registrierte Namen (DN), definiert 47
Registrierung
  Anpassung 8
  Benachrichtigungsschreiben 6
  Browser-Formulare 5
  Regel-Exits 6
  Systemvoraussetzungen 32
  Übersicht 5
  Vorabregistrierung 6
  Zertifikatstypen 6
Registrierungsdatenbank 5
Registrierungsdomäne
  Anpassung 8
  Beschreibung 5
  Definition 4
Registrierungsfunktion
  Anpassung 8
  Beschreibung 5
Registrierungsstelle (RA)
  Anpassung 8
  Client-Authentifizierung 44
  RA Desktop 7
  Regel-Exits 6
  Registrierung 5
  Übersicht 4
  unter AIX installieren 79
  unter Windows NT installieren 109
  Web-Server-Integration 13
  Zertifikatsprofile 6
Release-Informationen 27
Reservierte Datenbanknamen 43
Root-CA 11
Root-DN-Eintrag 48
rootvg, Datenträgergruppe 61
RS/6000 29
RS/6000-Server 29

S

S/MIME-Zertifikate 6
Schemaunterstützung 20
Schlüsselspeicher (KeyStores) 22
Schlüsselwiederherstellung 17
Selbstunterzeichnetes CA-Zertifikat 11
Seriennummern 10

Server-Konfigurationen 53
Server-Voraussetzungen
  erforderliche Hardware 29
  erforderliche Software 27
  für AIX 30
  für Windows NT 30
  wahlfreie Hardware 28
  wahlfreie Software 28
Server-Zertifikate 6
Setup Wizard
  Dokumentation 119
  Hilfe 120
  Swing Library 31
  Systemvoraussetzungen 31
  Übersicht 119
Sicherer Web-Server 44
Sicherheit
  Firewalls 41
  physisch 40
  System 40
Sicherheitshierarchie 11
Sicherung und Wiederherstellung, Schlüssel 17
Sicherungsabbilder
  AIX 64, 92
  NT 99, 117
Sicherungsmodell
  Codeunterzeichnung 21
  Datenverschlüsselung 22
  Nachrichtenunterzeichnung 21
  Schlüsselspeicher (KeyStores) 22
SMIT, Programm 61, 79
Softwarevoraussetzungen
  Directory-Server 28
  IBM 4758 PCI Cryptographic Coprocessor 28
  JDK 28
  Produkt-CD-ROMs 55
  Server, erforderlich 27
  Server, wahlfrei 28
  Setup Wizard 31
  Verteilung 55
  Web-Browser für Setup Wizard 31, 37
  Web-Server 28
Sprachen
  produktspezifische Unterschiede 54
  unterstützt 54
SSL-Protokoll 44
SSL-Zertifikate 6
Standards
  unter Tivoli PKI unterstützt 23
  Verschlüsselung 23
Standardzertifikatserweiterungen 24
Steuern des Server-Zugriffs 41
Swing Library 31
Systemabbild, konfigurieren 64
Systemarchitektur
  Diagramm 3
  Server-Konfigurationen 53
Systemdiagramm 3
Systemgröße
  für AIX empfohlen 30
  für Windows NT empfohlen 30
  Richtlinien 29
Systemschutz 40
Systemverwaltung
  Übersicht 122
  Zugriff 123
Systemvoraussetzungen
  Browser-Registrierung 32
  DB2 28
  Directory 28
  Hardware, Server 29
  IBM 4758 PCI Cryptographic Coprocessor 28
  RA Desktop 32
  Setup Wizard 31
  Software, Server 27
  wahlfreie Hardware, Server 28
  wahlfreie Software, Server 28
  Web-Server-Software 28

T

ta-backup, Dienstprogramm 92, 117
TCP/IP-Hostname prüfen 59
temp, Verzeichnis 96
Tivoli
  Kundenunterstützung xvi
  Webinformationen zur Sicherheitsverwaltung xvii

Tivoli *(Forts.)*
Websites für Sicherheitsprodukte xvii
Tivoli PKI
Webinformationen xvii
Tivoli PKI-Konfiguration, Benutzer 98
Tivoli PKI-System
Beschreibung 1
Datenbanksystem 14
Directory-Server 15
Funktionen 1
Haupt-Server 4
IBM 4758 PCI Cryptographic Coprocessor 15
Prüfsubsystem 12
RA-Server 4
Systemdiagramm 3
unter AIX installieren 77
unter Windows NT installieren 108
Verschlüsselungsstandards 23
Web-Server 13
Zertifikatsaussteller-Server 10

U

Überblick
verwendete Konventionen xvi
Überblick über die Vorgehensweise
AIX-Installation 57
Windows NT-Installation 96
Unicode-Unterstützung 54
Unterstützung, für Tivoli-Kunden xvi
Unterstützung in der Landessprache
Chiffrieralgorithmen 54
Encryption Edition 54
sprachenspezifische Unterschiede 54
Übersicht 54
URL-Adressen
IBM HTTP Server-Veröffentlichungen 46
Tivoli PKI-Bibliothek, Web-Seite xii
Tivoli PKI-Homepage xii
UTF-8-Verschlüsselung 54

V

Veröffentlichungen
Anpassung 126
Benutzerhandbuch 125
Beschreibung xii
Konfiguration 119
RA Desktop 123
Systemverwaltung 122
Tivoli-Sicherheitsprodukte xvii
Verschlüsselungsalgorithmen 54
Vorabregistrierung
Browser-Registrierung 6
Vorwort, Informationen xi
VPN-Zertifikate 6

W

Web-Server
DNS 45
HTTP-Protokoll 44
HTTPS-Protokoll 44
konfigurieren 44
öffentlicher Host 44
sichere Hosts 44
Softwarevoraussetzungen 28
SSL-Protokoll 44
Übersicht 13
unter AIX installieren 72
unter Windows NT installieren 101
Veröffentlichungen 46
Website für
Informationen zur Sicherheitsverwaltung xvii
Tivoli-Kundenunterstützung xvi
Tivoli Public Key Infrastructure xvii
Tivoli-Sicherheitsprodukte xvii
WebSphere Application Server
unter AIX installieren 72
unter Windows NT installieren 101, 104
WebSphere Application Server, Upgrade ausführen 75
Wiederherstellung, Schlüssel 17

Windows NT
Backup-Dienstprogramm 117
Betriebssystemversion 27
cfguser, Benutzername 43, 98
Directory-Server installieren 105
erforderliche Einstellungen 107
Hardwarekonfigurationen 30
Installationsabschluss, Prüfliste 116
Installationsrichtlinien 108
Installationsübersicht 96
IP-Aliasnamen 105
konfigurieren 96
Serverplattformen 27
Sicherheitsaspekte 40
Softwarevoraussetzungen 27
Überlegungen zur Firewall 41
Zugriffssteuerung 41

X

X.509v3-Zertifikate 24

Z

Zertifikate
Erweiterungen 25
Massenausstellung 18
selbst unterzeichnender CA 11
Sicherheitshierarchie 11
X.509v3-Unterstützung 24
Zertifikatsaussteller (CA)
Datenbank 10
DN-Eintrag 48
gegenseitige Zertifizierung 11
Hierarchie 11
IBM 4758 PCI Cryptographic Coprocessor 11, 15
Integration in den IBM 4758 PCI Cryptographic Coprocessor 49
Liste der ausgestellten Zertifikate 10
MACs 10
Zertifikatsaussteller (CA) *(Forts.)*
Schlüsselspeicher (KeyStore) 22
Schutz von Schlüsseln 49
selbstunterzeichnetes Zertifikat 11
Seriennummer 10
Speichern des Schlüssels in Hardware 50
Übersicht 10
unter AIX installieren 79
unter Windows NT installieren 109
Zertifikatswiderrufsliste 10
Zertifikatserweiterungen
allgemein 25
Anpassung 25
privat 25
Standard 24
unter Tivoli PKI 25
Zertifikatsprofile
Anpassung 8
Beschreibung 6
Zertifikatstypen 6
Zertifikatswiderrufsliste (CRL) 10
Zielgruppe xii
Zugriffssteuerung
CA-Berechtigungen 48
Directory-Administratorberechtigungen 48
Directory-Berechtigungen 48
Directory-Root-Berechtigung 48
RA Desktop-Berechtigungen 7
System 41

GC12-2916-01